ENTHEC©

kartos©

Soluciones de monitorización de amenazas externas

Estado, comparativa y futuro

Índice

INTRODUCCIÓN

En un mundo cada vez más interconectado, la ciberseguridad se ha convertido en una prioridad estratégica para las organizaciones de todos los sectores. Las amenazas externas, provenientes de actores malintencionados como ciberdelincuentes, grupos de espionaje industrial y estados nación, evolucionan constantemente, desafiando las defensas tradicionales y obligando a las empresas a adoptar enfoques más dinámicos y proactivos.

La **monitorización de amenazas externas** es una de las estrategias clave para anticiparse a los ataques y minimizar el impacto de posibles brechas de seguridad.

Las soluciones de monitorización de amenazas externas **permiten a las organizaciones identificar, analizar y mitigar riesgos en tiempo real,** proporcionando visibilidad sobre vulnerabilidades, intentos de ataque y posibles brechas antes de que se materialicen. Sin embargo, estas herramientas presentan desafíos significativos, como la necesidad de una integración eficiente con otros sistemas de seguridad, la gestión de alertas para reducir falsos positivos y la adaptación a nuevos vectores de ataque impulsados por tecnologías emergentes como la inteligencia artificial y la computación cuántica.

Este whitepaper tiene como objetivo **analizar el estado actual de las soluciones de monitorización de amenazas externas,** comparando sus características, capacidades y limitaciones, así como explorando su evolución futura en el contexto de la ciberseguridad empresarial. Para ello, se abordarán tecnologías clave como la inteligencia de amenazas (Threat Intelligence), la gestión de la Superficie Externa de Ataque (EASM), la estión del Riesgo Digital (DRPS) o la innovadora gestión continua de la exposición a amenazas (Continuous Threat Exposure Management, CTEM).

La necesidad de monitorizar las amenazas externas

En el entorno digital actual, las organizaciones enfrentan un panorama de amenazas en constante evolución. La proliferación de ciberataques, el aumento de vulnerabilidades y la sofisticación de los actores maliciosos han convertido la seguridad en un reto continuo. Ante esta realidad, la monitorización y gestión continua de la exposición a amenazas externas se ha vuelto imprescindible para las empresas que buscan minimizar riesgos y garantizar la resiliencia operativa.

EVOLUCIÓN DEL PANORAMA DE AMENAZAS EXTERNAS

Las amenazas externas han evolucionado significativamente en los últimos años. Los atacantes ya no se limitan a explotar vulnerabilidades conocidas, sino que emplean tácticas avanzadas como la inteligencia artificial, el ransomware dirigido y el phishing altamente personalizado.

Además, el auge del Internet de las Cosas (IoT) y la migración a entornos de nube han ampliado la superficie de ataque de las organizaciones, haciendo que la seguridad perimetral tradicional sea insuficiente.

Frente a este escenario, contar con una estrategia de monitorización continua permite detectar y responder rápidamente a posibles amenazas. Tecnologías como la Inteligencia de Amenazas, la Gestión Continua de la Exposición a Amenazas (Continuous Threat Exposure Management, CTEM) y las plataformas de correlación de eventos proporcionan visibilidad en tiempo real sobre la postura de seguridad de una organización.

BENEFICIOS DE UNA ESTRATEGIA DE GESTIÓN CONTINUA

Identificación temprana de riesgos:

La monitorización continua permite descubrir vulnerabilidades antes de que sean explotadas por atacantes. Herramientas avanzadas de escaneo y evaluación de riesgos ayudan a priorizar los problemas más críticos y a tomar decisiones informadas.

Reducción del tiempo de respuesta:

Las soluciones de detección de amenazas en tiempo real facilitan una reacción rápida ante actividades sospechosas, minimizando el impacto de incidentes de seguridad.

Cumplimiento normativo:

Regulaciones como el RGPD, la ISO 27001 y el NIST exigen a las organizaciones mantener una vigilancia constante sobre su seguridad. Implementar una estrategia de CTEM facilita el cumplimiento normativo y reduce el riesgo de sanciones por incumplimiento.

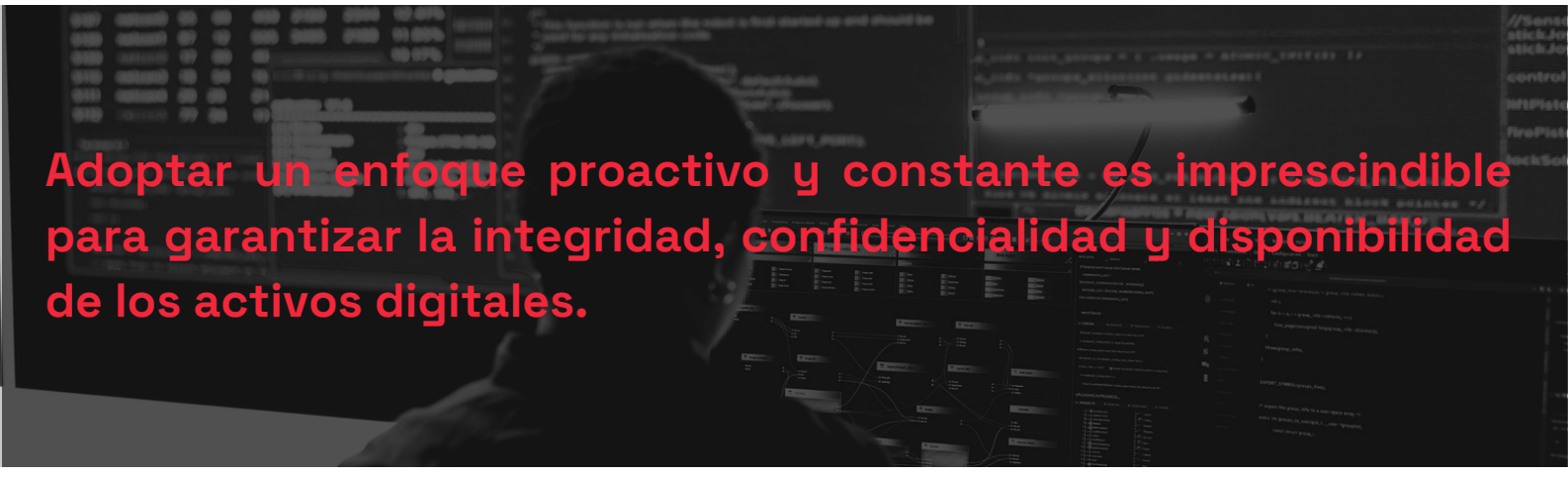
Mejora en la toma de decisiones:

La correlación de datos de amenazas externas con información interna proporciona una visión integral de los riesgos. Esto permite a los equipos de seguridad ajustar su estrategia de protección de manera proactiva.

DATOS:

La incidencia de ataques relacionados con phishing, el fraude y la estafa subió tres puntos porcentuales en 2023 respecto al año anterior, representando la mayor subida entre las diferentes amenazas.

*Identity Theft Resource Center (ITRC): 2023 Business Impact Report



- El panorama de amenazas cambia rápidamente. Los ciberdelincuentes evolucionan sus tácticas, técnicas y procedimientos a un ritmo vertiginoso, lo que hace que las medidas de seguridad estáticas se queden obsoletas en poco tiempo. La monitorización continua permite **detectar amenazas en tiempo real,** identificando posibles ataques antes de que causen daños irreparables. Este nivel de vigilancia constante solo puede lograrse mediante el uso de **herramientas avanzadas de análisis de seguridad, inteligencia artificial y machine learning.** La gestión proactiva de amenazas no solo consiste en detectar ataques, sino también en anticiparse a ellos. Esto implica realizar evaluaciones de riesgo periódicas, aplicar parches de seguridad de manera continua y capacitar a los empleados para reconocer intentos de phishing o ingeniería social.

- En este contexto, las tecnologías de monitorización de las amenazas externas, como las de Gestión Continua de la Exposición a Amenazas (Continuous Threat Exposure Management, CTEM) juegan un papel crucial. **La monitorización permite a las organizaciones identificar, evaluar y mitigar continuamente vulnerabilidades y exposiciones antes de que sean explotadas por atacantes.** Estas soluciones proporcionan visibilidad en tiempo real sobre los puntos débiles de la infraestructura, priorizando las amenazas más críticas con base en el impacto potencial.

- La integración de las soluciones de cibervigilancia con SIEM y EDR resulta esencial para lograr una estrategia de ciberseguridad eficaz y coordinada. Un SIEM recopila y analiza registros de eventos de diversas fuentes dentro de la infraestructura, permitiendo la correlación de datos en tiempo real. Cuando se integra con las soluciones de monitorización de amenazas externas, se **mejora la visibilidad sobre los riesgos en la superficie de ataque y se pueden generar alertas priorizadas según la criticidad de las vulnerabilidades detectadas**. Por otro lado, un EDR proporciona monitoreo y respuesta avanzada en endpoints, permitiendo a las organizaciones reaccionar de manera rápida ante amenazas activas. Al conectar EDR con CTEM, se mejora la capacidad de mitigación al recibir inteligencia de amenazas contextualizada, lo que permite aplicar medidas de contención antes de que un ataque escale.

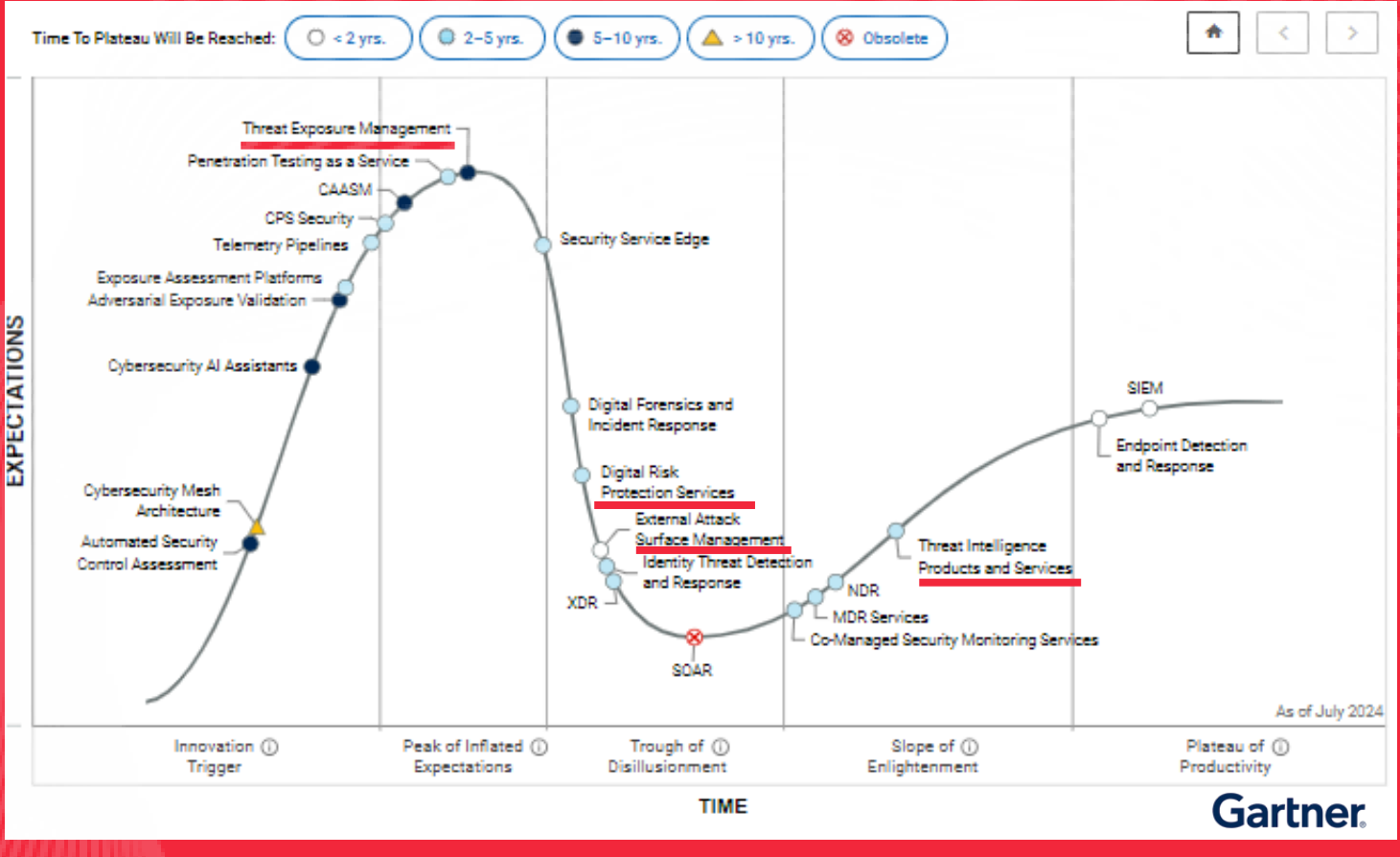
Tipos de soluciones de monitorización de amenazas externas

La monitorización de amenazas externas abarca un conjunto diverso de soluciones diseñadas para detectar riesgos fuera del perímetro de la organización. Estas herramientas varían el enfoque, alcance y nivel de automatización, adaptándose a distintas necesidades y entornos.

- **Soluciones de Threat Intelligence**
- **Soluciones de Gestión de la Superficie Externa de Ataque (EASM)**
- **Soluciones de Gestión del Riesgo Digital (DRPS)**
- **Soluciones de Gestión Continua de la Exposición a Amenazas (CTEM)**

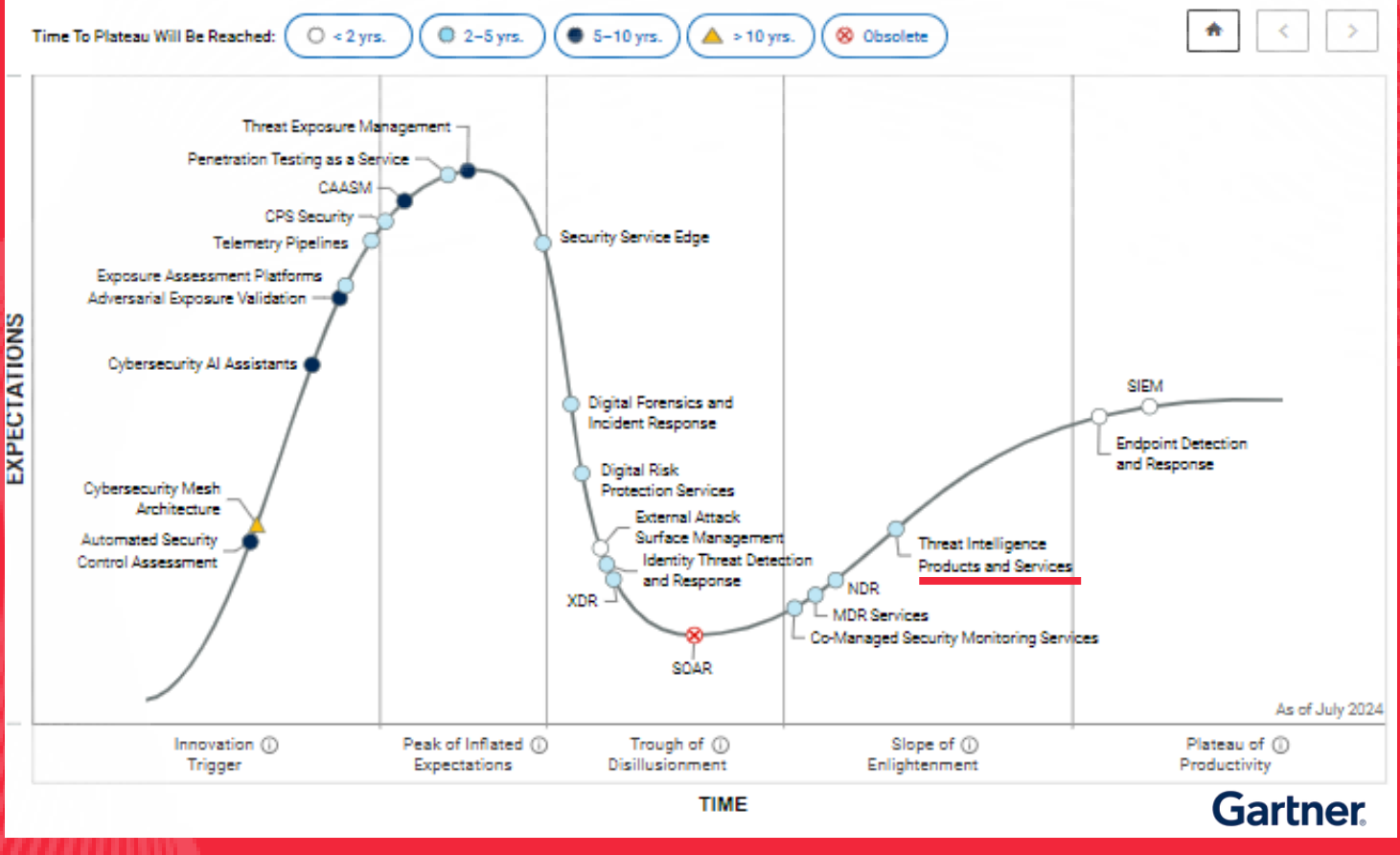
TIPOS DE SOLUCIONES DE MONITORIZACIÓN DE AMENAZAS EXTERNAS

Dentro del ciclo de vida de herramientas de ciberseguridad utilizadas actualmente, Gartner incluye cuatro soluciones de monitorización de amenazas externas:



- **Soluciones de Threat Intelligence**
- **Soluciones de Gestión de la Superficie Externa de Ataque (EASM)**
- **Soluciones de Gestión del Riesgo Digital (DRPS)**
- **Soluciones de Gestión Continua de la Exposición a Amenazas (CTEM)**

THREAT INTELLIGENCE



THREAT INTELLIGENCE

• ¿Qué es?

La **Inteligencia de Amenazas (Threat Intelligence)** es el proceso de recopilar, analizar y utilizar información sobre amenazas potenciales o existentes que pueden afectar a una organización. Su objetivo es proporcionar datos procesables que ayuden a mejorar la seguridad informática y prevenir ataques.

- Permite conocer el entorno de amenazas, proporcionando información sobre actores maliciosos, tácticas utilizadas, vulnerabilidades explotadas y posibles objetivos.
- Ayuda a identificar patrones en ataques previos para anticipar futuros riesgos.

Inteligencia estratégica:
Información de alto nivel utilizada por directivos y responsables de seguridad para tomar decisiones sobre inversiones en ciberseguridad y políticas de protección

Inteligencia táctica:
Datos sobre las tácticas, técnicas y procedimientos (TTP) utilizados por los atacantes. Es útil para los equipos de seguridad informática que gestionan la infraestructura.

Inteligencia operacional:
Información detallada sobre ataques en curso, direcciones IP maliciosas, dominios sospechosos y patrones de actividad delictiva en la red.

• ¿Cómo funciona?

Recopilación de datos:
Obtienen información de diversas fuentes como bases de datos de amenazas, foros en la dark web, registros de ataques previos y redes de sensores.

Análisis de datos:
Aplican algoritmos de inteligencia artificial y machine learning para identificar patrones sospechosos.

Correlación de eventos:
Relacionan eventos de seguridad con información de amenazas conocidas para detectar posibles incidentes.

Generación de alertas:
Notifican sobre tendencias de actividades sospechosas o indicadores de compromiso (IoC) que puedan representar una amenaza.

THREAT INTELLIGENCE

• Ventajas

1. Identificación tendencias de amenazas

Detección de tendencias de amenazas por países y sectores para adecuar la estrategia y los recursos a defenderse frente a ellas.

2. Reducción del tiempo de respuesta ante un incidente y de daños.

Gracias a la estrategia de ciberseguridad elaborada en base a los datos proporcionados por la Inteligencia de Amenazas, se reducen los tiempos de respuesta y se refuerza la mitigación de daños.

3. Mejora de la toma de decisiones

Con datos basados en Inteligencia de Amenazas, las organizaciones pueden asignar mejor sus recursos y priorizar acciones de mitigación.

4. Protección contra amenazas avanzadas

Los ciberataques evolucionan constantemente, y muchas técnicas sofisticadas identificadas por la Inteligencia de Amenazas pasarían desapercibidas para los sistemas de defensa tradicionales.

5. Cumplimiento normativo

Facilita el cumplimiento al proporcionar visibilidad sobre las amenazas y garantizar una respuesta eficaz.

6. Reducción de costes

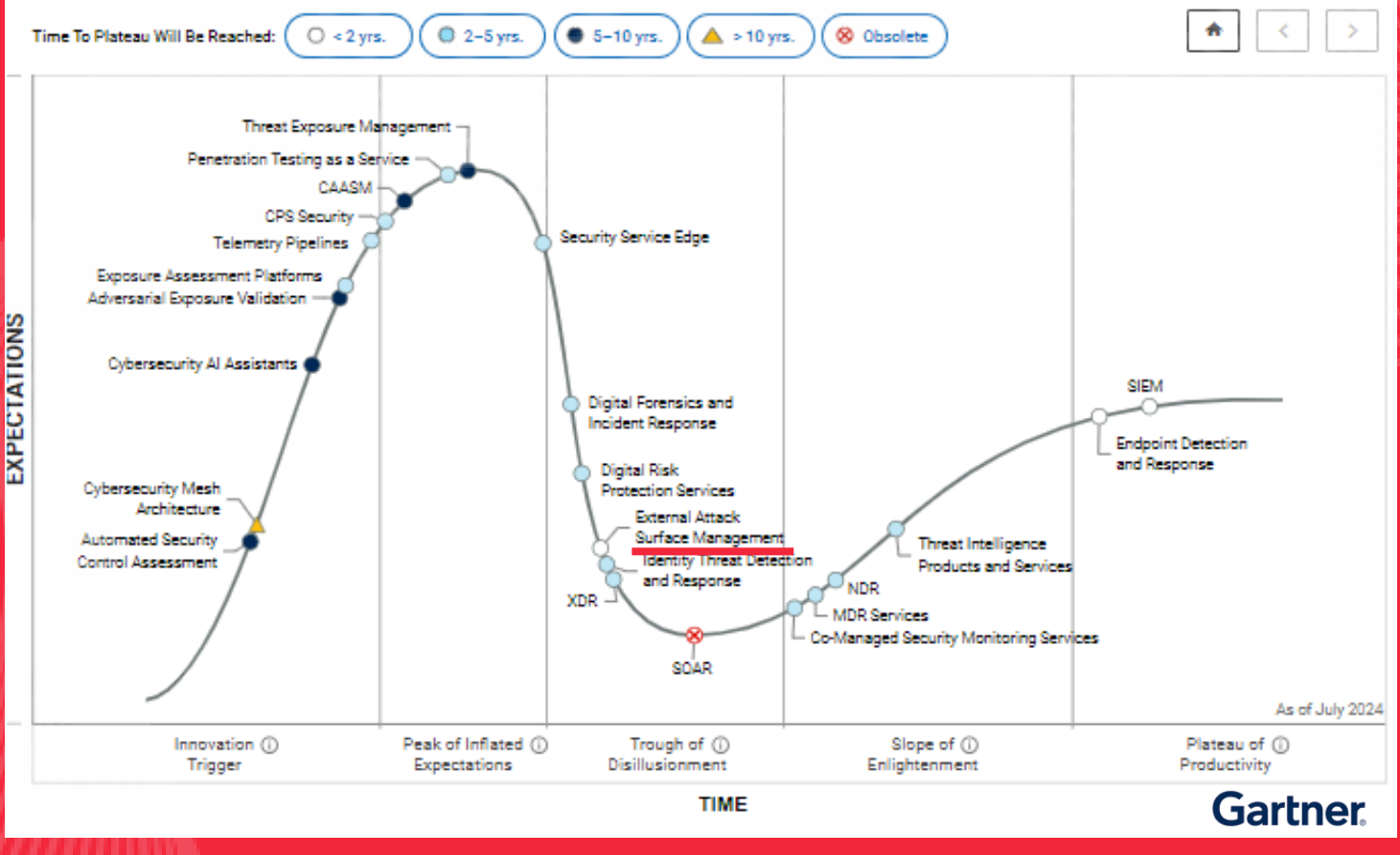
Ayuda a evitar pérdidas financieras derivadas de ciberataques, daños a la reputación y sanciones regulatorias.

THREAT INTELLIGENCE

• Threat Intelligence frente al resto

⊕	• Herramienta transversal, que da información en tiempo real sobre ataques en el mundo y por sectores. • Buena para conocer el estado general del entorno en materia de ciberseguridad y diseñar estrategias.
⊖	• No da información sobre los riesgos o ataques en curso de una organización concreta. • Mala para la protección inmediata y continua de la organización frente a riesgos propios en curso.

GESTIÓN DE LA SUPERFICIE EXTERNA DE ATAQUE (EASM)



GESTIÓN DE LA SUPERFICIE EXTERNA DE ATAQUE (EASM)

¿Qué es?

La **superficie de ataque externa** incluye todos los activos digitales de una organización que están accesibles desde internet. Esto abarca sitios web, servidores en la nube, APIs, dominios, direcciones IP y otros sistemas conectados que pueden ser potencialmente explotados por ciberdelincuentes.

- Ayuda a las organizaciones a **descubrir, evaluar y gestionar** estos activos expuestos, permitiéndoles reducir los riesgos antes de que sean explotados por atacantes.
- Proporcionan visibilidad en tiempo real sobre los activos externos y permiten **priorizar vulnerabilidades** para mejorar la seguridad.

¿Cómo funciona?

Descubrimiento de activos digitales:

- Identifica automáticamente todos los activos digitales de la organización, incluyendo aquellos desconocidos o no gestionados.
- Escanea dominios, subdominios, direcciones IP, aplicaciones web y APIs expuestas.

Análisis de vulnerabilidades:

- Evalúa si los activos detectados tienen vulnerabilidades de seguridad, configuraciones incorrectas o software desactualizado.
- Aplica metodologías de hacking ético y pruebas de penetración automatizadas para identificar riesgos.

Monitorización continua:

- Escanea en tiempo real para detectar cambios en la superficie de ataque, como la aparición de nuevos activos o exposiciones accidentales.
- Alerta sobre nuevos riesgos para una rápida mitigación.

Evaluación de riesgos y priorización

- Utiliza algoritmos de análisis de riesgos para clasificar las amenazas en función de su criticidad.
- Permite a las organizaciones centrarse en los problemas más graves y urgentes.

GESTIÓN DE LA SUPERFICIE EXTERNA DE ATAQUE (EASM)

- **Ventajas**

1. Mayor visibilidad sobre la superficie de ataque
Visión completa y actualizada de los sistemas accesibles desde internet, incluyendo aquellos que podrían haber sido olvidados o mal gestionados.

2. Detección temprana de vulnerabilidades
Prevención incidentes como ataques de ransomware, robo de datos o acceso no autorizado a sistemas críticos.

3. Reducción del riesgo de ataques cibernéticos
Reducción de posibilidades de que los ciberdelincuentes logren explotar fallos de seguridad.

4. Cumplimiento normativo y regulatorio
Las últimas normativas de ciberseguridad, requieren que las organizaciones de sectores sensibles gestionen adecuadamente su superficie de ataque.

5. Optimización del tiempo y recursos del equipo de seguridad
Automatización de tareas que de otro modo requerirían mucho tiempo, como el mapeo de activos y la detección de vulnerabilidades.

6. Integración con otras herramientas de ciberseguridad
Puede integrarse con otras plataformas de seguridad, como firewalls, herramientas de Threat Intelligence y sistemas de detección de intrusos (IDS/IPS). Esto permite una defensa más coordinada y efectiva.

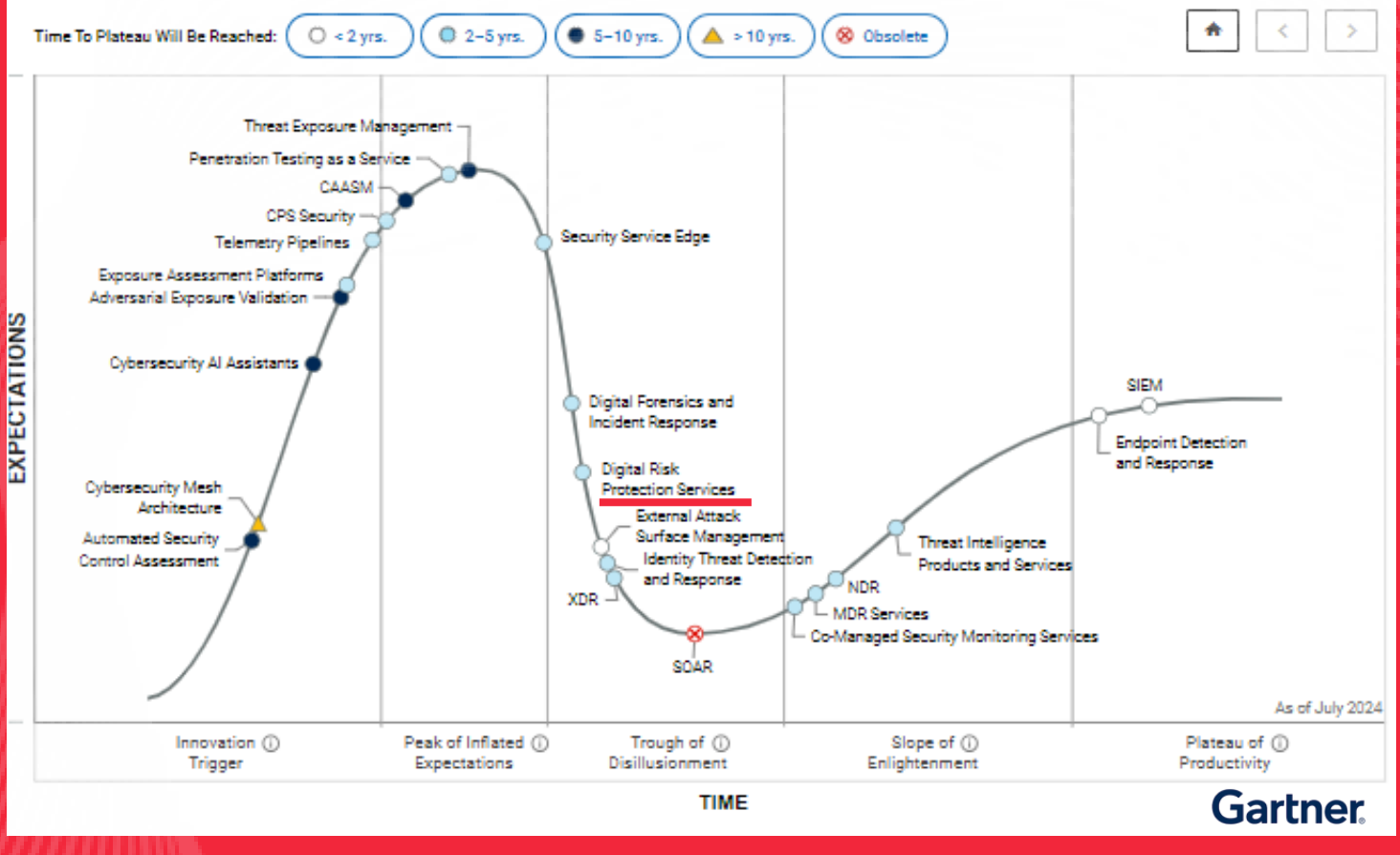
7. Respuesta proactiva a incidentes de seguridad
Las organizaciones pueden actuar de forma proactiva ante posibles amenazas, en lugar de reaccionar después de que ocurra un ataque.

GESTIÓN DE LA SUPERFICIE EXTERNA DE ATAQUE (EASM)

- **EASM frente al resto**

⊕	• Analiza los agujeros y las vulnerabilidades que existen en los elementos físicos de la infraestructura de las compañías, tales como servidores expuestos, webs, redes, o elementos orientados a Internet, que pueden terminar en un ciberataque. • Analiza y prioriza cuáles son los riesgos y cuáles son aquellos elementos que son más susceptibles de sufrir un ataque o de ser explotados por cibercriminales. • En algunos casos, mediante la integración con terceros o incluso con tecnología propia, pueden ofrecer funcionalidades de mitigación y remediación
⊖	• Funciona generalmente de forma intrusiva, ya que son herramientas internas que vigilan desde dentro la superficie externa. • Sus capacidades están limitadas a localizar fallos de infraestructura del perímetro.

GESTIÓN DEL RIESGO DIGITAL (DRPS)



GESTIÓN DEL RIESGO DIGITAL (DRPS)

• ¿Qué es?

La **superficie de ataque externa** incluye todos los activos digitales de una organización que están accesibles desde internet. Esto abarca sitios web, servidores en la nube, APIs, dominios, direcciones IP y otros sistemas conectados que pueden ser potencialmente explotados por ciberdelincuentes.

- Ayuda a las organizaciones a **descubrir, evaluar y gestionar** estos activos expuestos, permitiéndoles reducir los riesgos antes de que sean explotados por atacantes.
- Proporcionan visibilidad en tiempo real sobre los activos externos y permiten **priorizar vulnerabilidades** para mejorar la seguridad.

• ¿Cómo funciona?

Descubrimiento de activos digitales:

- Identifica automáticamente todos los activos digitales de la organización, incluyendo aquellos desconocidos o no gestionados.
- Escanea dominios, subdominios, direcciones IP, aplicaciones web y APIs expuestas.

Análisis de vulnerabilidades:

- Evalúa si los activos detectados tienen vulnerabilidades de seguridad, configuraciones incorrectas o software desactualizado.
- Aplica metodologías de hacking ético y pruebas de penetración automatizadas para identificar riesgos.

Monitorización continua:

- Escanea en tiempo real para detectar cambios en la superficie de ataque, como la aparición de nuevos activos o exposiciones accidentales.
- Alerta sobre nuevos riesgos para una rápida mitigación.

Evaluación de riesgos y priorización

- Utiliza algoritmos de análisis de riesgos para clasificar las amenazas en función de su criticidad.
- Permite a las organizaciones centrarse en los problemas más graves y urgentes.

GESTIÓN DEL RIESGO DIGITAL (DRPS)

- **Ventajas**

1. Detección temprana de amenazas
Permite a las organizaciones identificar riesgos antes de que sean explotados, lo que reduce el impacto de los ataques y mejora la capacidad de respuesta.

2. Protección contra la filtración de datos
Ayuda a detectar credenciales robadas, información sensible comprometida o bases de datos filtradas, permitiendo tomar acciones rápidas para proteger la organización.

3. Reducción del riesgo de fraude y phishing
Ayuda a detectar sitios web fraudulentos y cuentas falsas que buscan engañar a clientes y empleados.

4. Protección de la reputación de la empresa
Control de la imagen de la organización en el entorno digital, evitando que ataques de desinformación o suplantaciones dañen su reputación.

5. Mejora de la resiliencia corporativa frente a ataques
Ayuda a fortalecer la resiliencia de la empresa frente a ciberataques.

6. Cumplimiento normativo y regulatorio
Facilita el cumplimiento legal al detectar incidentes de seguridad y generar reportes de riesgos.

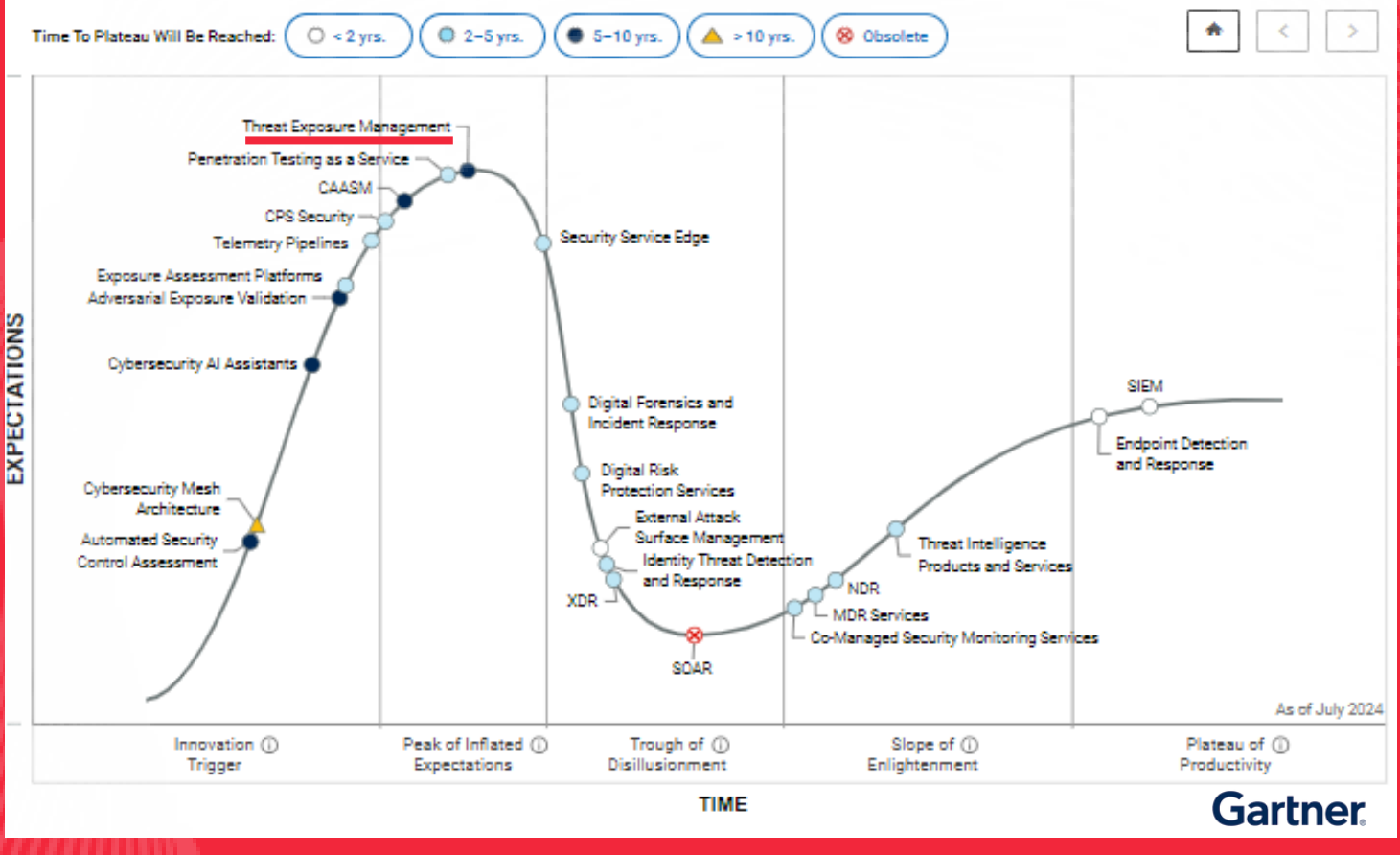
7. Integración con otros sistemas de seguridad
Puede integrarse con Threat Intelligence, SIEM y plataformas de respuesta a incidentes, mejorando la capacidad de detección y mitigación de amenazas.

GESTIÓN DEL RIESGO DIGITAL (DRPS)

• DRPS frente al resto

⊕	• Protege los activos digitales, es decir, la información de la organización que está expuesta fuera de su perímetro y que es visible para terceros. • Evalúa el riesgo de marca, verifica si hay información, credenciales, o datos filtrados, incluso huecos y fallos que puedan verse desde el exterior. • En muchos casos permite también la monitorización de la información de personas de interés, sean VIP, ejecutivos, o personas relevantes de la empresa.
⊖	• No abarca la localización de brechas existentes en los elementos físicos de la infraestructura de la compañía ni el inventario de activos y sistemas que están expuestos al exterior.

GESTIÓN CONTINUA DE LA EXPOSICIÓN A AMENAZAS (CTEM)



GESTIÓN CONTINUA DE LA EXPOSICIÓN A AMENAZAS (CTEM)

• ¿Qué es?

La **Gestión Continua de la Exposición a Amenazas (CTEM)** es un enfoque de seguridad que permite a las organizaciones **evaluar y reducir constantemente su superficie de ataque.**

- Permite mantener una **visión en tiempo real** de las vulnerabilidades y riesgos, capacitando para responder de manera más rápida y eficiente a las amenazas emergentes.
- No solo busca detectar fallos de seguridad, sino que también ayuda a **priorizar y gestionar la corrección de las vulnerabilidades** en función de su impacto potencial.

• ¿Cómo funciona?

1. Identificación de activos expuestos

- Escanea y analiza continuamente los activos digitales de la organización.
- Detectan sistemas, aplicaciones y servicios que podrían ser explotados por ciberdelincuentes.

2. Evaluación de vulnerabilidades

- Identifica fallos de seguridad en software, configuraciones incorrectas o credenciales expuestas.
- Utiliza inteligencia de amenazas para determinar qué vulnerabilidades son más propensas a ser explotadas.

3. Priorización de riesgos

- Clasifica las vulnerabilidades en función de su nivel de criticidad y probabilidad de explotación.
- Proporciona recomendaciones accionables para remediar los riesgos más urgentes.

4. Monitoreo y respuesta en tiempo real

- Detecta nuevos riesgos de manera continua, sin necesidad de auditorías programadas.
- Takedowns y alertas en tiempo real a los equipos de seguridad sobre hallazgos y cambios en la exposición a amenazas.

GESTIÓN CONTINUA DE LA EXPOSICIÓN A AMENAZAS (CTEM)

- **Ventajas**

1.Unificación de varias soluciones de monitorización en una

Simplificación de los procesos de monitorización y gestión de vulnerabilidades, ya que unifican capacidades de ciberseguridad como EASM, DRPS, scoring, monitorización de terceros y protección de VIPs en una sola herramienta.

2. Evaluación continua de la superficie de ataque

Visión constante y actualizada de la exposición a amenazas, incluidas las de la cadena de valor.

3. Priorización de amenazas críticas

Ayuda a priorizar los riesgos más peligrosos en función de su impacto potencial y su probabilidad de explotación.

4. Reducción del tiempo de respuesta ante incidentes

Permite actuar más rápidamente para mitigar riesgos, reduciendo el tiempo en que una vulnerabilidad permanece expuesta.

5. Integración con otras herramientas de seguridad

Integración con sistemas de gestión de incidentes, inteligencia de amenazas y análisis forense, mejorando la coordinación en la respuesta ante ataques.

6. Reducción del riesgo de brechas de seguridad

Ayuda a prevenir incidentes de seguridad antes de que ocurran.

7. Adaptación a las nuevas amenazas

Permite que las empresas se adapten en tiempo real a nuevas tácticas de ataque y técnicas de explotación y controlar su impacto en la seguridad corporativa.

8. Cumplimiento normativo y auditorías de seguridad

Facilita el cumplimiento de regulaciones de ciberseguridad, proporcionando en tiempo real informes detallados sobre la gestión de riesgos y la mitigación de vulnerabilidades de las organizaciones.

9. Foco en el impacto en el negocio

Permite orientar la estrategia de ciberseguridad a criterios de negocio, facilitando la priorización de los riesgos y la atención a determinadas vulnerabilidades, atendiendo al posible impacto en el negocio, conociendo la probabilidad de un ataque y a qué parte de la compañía afectaría.

GESTIÓN CONTINUA DE LA EXPOSICIÓN A AMENAZAS (CTEM)

- **CTEM frente al resto**

⊕	• Integración de todos los tipos de herramientas anteriores para obtener una monitorización automatizada, continua y en tiempo real orientada a criterios de negocio. • Capacidad de monitorizar de forma continua, automatizada y en tiempo real la superficie externa de ataque, el riesgo digital, el riesgo de terceros, la protección de personas relevantes de la organización, el compliance propio y de terceros, así como el impacto de la inteligencia artificial. • Permite a la organización priorizar los riesgos y la atención a determinadas vulnerabilidades y determinados problemas, atendiendo no solo a criterios técnicos, sino también de negocio.
⊖	• Poco tiempo en el mercado y pocos fabricantes ofreciendo este tipo de herramientas. • Escaso conocimiento de la existencia de esta tecnología avanzada por parte de los equipos de ciberseguridad corporativos. • Innovación tecnológica constante para no quedar obsoleta.

GESTIÓN CONTINUA DE LA EXPOSICIÓN A AMENAZAS (CTEM)

• Gartner sobre CTEM

Gartner destaca la **Gestión Continua de la Exposición a Amenazas (CTEM)** como una tendencia clave en ciberseguridad. . Su enfoque permite a las organizaciones evaluar de manera continua la accesibilidad, exposición y explotabilidad de sus activos digitales y físicos. A diferencia de las evaluaciones periódicas tradicionales, CTEM ofrece una visión constante y actualizada de las vulnerabilidades, facilitando una respuesta más ágil y efectiva ante posibles amenazas.

Gartner enfatiza que, con la expansión de las superficies digitales de ataque y de la influencia de la IA en la ejecución de los ciberataques, los modelos de ciberseguridad tradicionales, centrados en parchear y asegurar sistemas físicos y software autogestionado, ya no son suficientes. CTEM ofrece el enfoque completo y proactivo que es necesario en la actualidad.

Además, Gartner predice que, **para 2026, las superficies de ataque no parcheables habrán crecido, representando más de la mitad de la empresa.** Por lo tanto, los programas tradicionales de gestión de vulnerabilidades no podrán mantenerse día, y se espera que las organizaciones que prioricen las inversiones en seguridad basadas en CTEM tengan tres veces menos probabilidades de sufrir una brecha de seguridad.

Por todo ello, Gartner considera que la adopción de CTEM, y la utilización de las soluciones de monitorización necesarias, es esencial para que las organizaciones mantengan una postura de seguridad sólida y proactiva frente a las amenazas cibernéticas emergentes.

kartos®

El futuro de la protección frente a las amenazas

El panorama de la ciberseguridad está en constante evolución, y las organizaciones deben adaptarse para protegerse eficazmente contra amenazas externas.

El futuro de la protección frente a las amenazas

1. IA y aprendizaje automático

La aplicación de la inteligencia artificial (IA) y el aprendizaje automático (ML) en ciberseguridad supone un riesgo, pero también está revolucionando la forma en que las organizaciones detectan y responden a las amenazas. Estas tecnologías permiten analizar grandes volúmenes de datos para identificar patrones y anomalías que indican actividades maliciosas, facilitando una respuesta más proactiva y eficiente.

2. Enfoque Zero Trust

El modelo de seguridad Zero Trust, basado en el principio de "nunca confiar, siempre verificar", seguirá ganando tracción. Este enfoque implica que ninguna entidad, ya sea interna o externa, es considerada confiable por defecto. Cada solicitud de acceso debe ser autenticada y autorizada, lo que ayuda a prevenir amenazas internas y externas.

3. Aumento de ataques en la cadena de suministro

Se anticipa un incremento en los ataques dirigidos a las cadenas de suministro. Los ciberdelincuentes buscan vulnerabilidades en proveedores o socios para infiltrarse en organizaciones objetivo. Esto subraya la necesidad de una gestión de riesgos más rigurosa un mayor control sobre terceros para garantizar la seguridad en toda la cadena.

4. Expansión de la Superficie de Ataque

Con la digitalización y la adopción de tecnologías emergentes, la superficie de ataque de las organizaciones se está ampliando. Esto incluye dispositivos IoT, entornos de nube y sistemas remotos, que requieren estrategias de seguridad más integrales y actualizadas para proteger todos los puntos de entrada potenciales.

5. Criptografía Post-Cuántica

La llegada de la computación cuántica plantea desafíos para los métodos criptográficos actuales. Las organizaciones deberán prepararse adoptando técnicas de criptografía post-cuántica para proteger sus datos contra posibles amenazas futuras derivadas de esta tecnología emergente.

6. España como líder emergente

España se está posicionando como un líder emergente en ciberseguridad en Europa, gracias a inversiones significativas y al desarrollo de talento especializado, volcado en el diseño de soluciones y herramientas avanzadas de ciberseguridad estratégica.

kartos©

Kartos Corporate Threat Watchbots es la plataforma CTEM desarrollada por Enthec que localiza la información y vulnerabilidades corporativas expuestas que pueden ser explotadas para ejecutar un ataque, para que las organizaciones puedan protegerse y mejorar sus defensas.

CiberInteligencia

Para descubrir vulnerabilidades latentes

Localiza la información y las vulnerabilidades abiertas y expuestas de la empresa en Internet, la Deep Web, Dark Web y las Redes Sociales. Campañas de phishing, fraude y estafas, CVEs y salud de DNS. Contraseñas y credenciales filtradas, documentación o bases de datos.

Ciberseguridad

Para mantener seguros los activos digitales

Expande la estrategia de ciberseguridad más allá del perímetro de IT corporativo. Protección de marca, dominio y subdominios. Protección de correo electrónico corporativo. Protección contra ransomware. Seguridad web y eliminación de amenazas.

Scoring

Para aumentar la puntuación de seguridad

Puntuación de ciberseguridad corporativa y de terceros basada en datos objetivos tomados en tiempo real.

Compliance

Para cumplir con las regulaciones actuales

Cumplimiento corporativo y de terceros basado en datos objetivos tomados en tiempo real. ISO 27001. PCI-DSS.

POR QUÉ ELEGIR KARTOS

- Monitorización automatizada, no intrusiva y continua.
- 5 herramientas en una: EASM, DRPS, Scoring, Riesgo de Terceros y Protección de VIPs.
- Alertas en tiempo real sobre vulnerabilidades abiertas y expuestas.
- Eliminación de falsos positivos en los resultados de búsqueda gracias a las Etiquetas de Contexto de Kartos, que utilizan IA desarrollada internamente.
- Sin back doors, el desarrollo de toda la tecnología utilizada por Kartos es interno y no dependemos de aplicaciones de terceros para su funcionamiento.
- Para empezar a trabajar, Kartos solo necesita la introducción del dominio a monitorizar. No se requiere implementación en el sistema de IT de la organización.
- Precio anual de las licencias cerrado.

ENTHEC©

#WeAlreadyKnow

ENTHEC©

@enthec

@enthecsolutions

kartos©