CEQUENCE

Ficha de dato

Protección API unificada de Cequence

Introducción DESCUBRIMIENTO

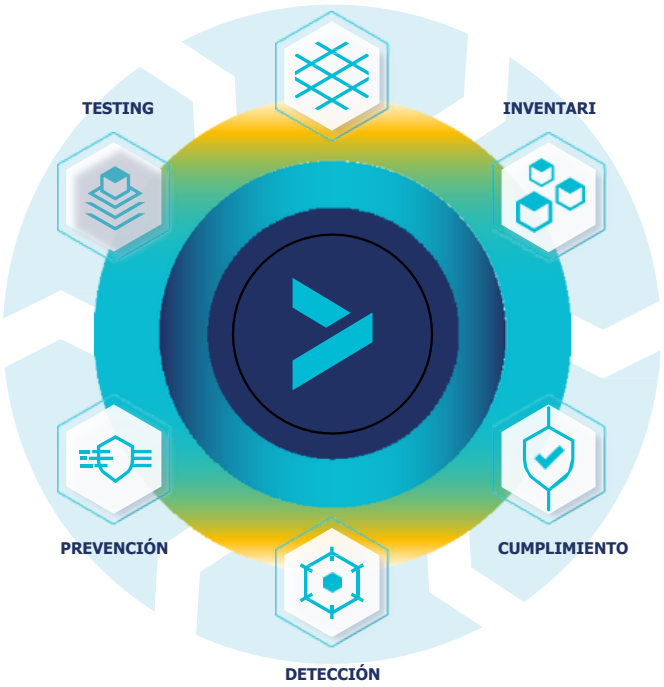
Las API se han convertido en la moneda de cambio de todo lo que hacemos digitalmente. Las aplicaciones que usamos en nuestros dispositivos para el trabajo y el placer, nuestro sitio web favorito de compras, administración de dinero y viajes, utilizan API en gran medida. Las organizaciones de todos los tamaños utilizan las API para aumentar la velocidad del negocio y crear una ventaja competitiva.

Al igual que con todas las cosas digitales, abundan los riesgos de seguridad, y las API no son una excepción: son puertas de entrada muy visibles y bien definidas a los datos y procesos comerciales de una organización. Con demasiada frecuencia, carecen de suficientes medidas de seguridad y se han convertido en el objetivo de ataque número 1. Para garantizar el éxito comercial, los equipos de seguridad deben evitar el uso indebido y el abuso que pueden conducir al fraude, la pérdida de datos y la interrupción del negocio en sus API, así como en sus aplicaciones web y móviles heredadas.

Desafíos de seguridad de API

Los equipos de seguridad de hoy carecen de las capacidades de visibilidad y defensa necesarias para proteger sus API de ataques contra API perfectamente codificadas y de explotaciones de vulnerabilidades causadas por errores de codificación lanzados a producción. Muchos han adoptado la creencia de que el cumplimiento de PCI o SOC 2 combinado con un cambio a la izquierda, la mentalidad DevOps respaldada por las tecnologías de seguridad existentes es suficiente para identificar su superficie de riesgo de API y ejercer más controles de administración y seguridad.

El problema con estas estrategias es que no tienen una forma de "conocer lo desconocido", lo que significa que no pueden buscar todas las API y vulnerabilidades de API sin saber dónde buscar. Incluso si todas las API se descubren y se "conocen", los atacantes aún pueden aprovechar transacciones aparentemente legítimas en un intento de robar datos o cometer fraude. Los enfoques tradicionales que utilizan WAF o puertas de enlace API dependen de una detección fácilmente evadible, carecen de tiempo para discernir la actividad API buena de la mala y dependen de la protección estática del mínimo común denominador distribuida en múltiples componentes tecnológicos.



La solución ideal: Protección API unificada

La solución ideal es aquella que aborde cada fase del ciclo de vida de seguridad de su API, que se pueda implementar rápidamente sin instrumentación o agentes intrusivos, y que se escale fácilmente. La solución debe proporcionar una vista de afuera hacia adentro y de adentro hacia afuera de la superficie de riesgo de la API, permitir el descubrimiento y la corrección de vulnerabilidades dinámicas mientras aprovecha el aprendizaje automático y la inteligencia de amenazas para:

- Descubra las API y los recursos de cara al público, creando un inventario en tiempo de ejecución de sus API administradas, no administradas, ocultas y zombis.
- Detecte vulnerabilidades antes de que se conviertan en exploits, descubra el abuso de la lógica empresarial y las amenazas de API que se ocultan a plena vista.
- Mitigue las amenazas con pruebas de API y tareas de remediación mientras bloquea los ataques de forma nativa, en tiempo real, sin señalar una solución de terceros.

The Cequence Unified API Protection solution is just that.

Protección API Unificada de Cequence

La única oferta que aborda todas las fases del ciclo de vida de la seguridad de su API, protege sus API de los atacantes y elimina los riesgos de seguridad de API desconocidos y no mitigados que conducen a la pérdida

	Cequence API Spyder	Cequence API Sentinel	Cequence API Spartan
API Descubrimiento	✓		
API Inventario		✓	
API Descubrimiento		✓	
API Testing de Seguridad		✓	
Threat Detección			✓
Threat Prevención			✓

La solución Cequence Unified API Protection está compuesta:

API Spyder.

Una herramienta de administración y descubrimiento de superficie de ataque de API que evalúa continuamente sus API y recursos públicos para mostrarle exactamente lo que ve un atacante desde afuera hacia adentro perspectiva. API Spyder descubre recursos de API de cara al público que pueden explotarse mediante vulnerabilidades como Log4j y LoNg4j.

API Sentinel

Proporciona una vista de adentro hacia afuera de sus API al integrarse con cualquier elemento de infraestructura de red para crear un catálogo actualizado de todas sus API, administradas y no administradas. Predefinido Las reglas de evaluación de riesgos ayudan a descubrir errores de codificación de cumplimiento de especificaciones, autenticación y manejo de datos confidenciales.

API Testing de Seguridad

Proporciona a los equipos de seguridad y desarrollo una combinación de pruebas de API predefinidas, importadas o generadas dinámicamente que van más allá del **OWASP API Security Top 10+** para ayudarlos a descubrir y remediar rápidamente las vulnerabilidades de la API. Vea y comparta el estado de las pruebas, los informes resumidos e inicie alertas por correo electrónico, webhooks y otras herramientas de colaboración populares.

API Spartan

Detecta y previene ataques de API automatizados sofisticados y abuso de lógica empresarial utilizando cientos de reglas de ML que aprovechan una base de datos de amenazas de API con miles de millones de comportamientos maliciosos, direcciones IP
y organizaciones. Las opciones de respuesta nativas basadas en políticas aseguran que cualquier ataque detectado se bloquee, en tiempo real, sin depender de un WAF de terceros u otro componente de seguridad.

La solución Cequence Unified API Protection está impulsada por un motor de análisis basado en ML que aprovecha la mayor base de datos de amenazas de API de patrones de comportamiento, infraestructura maliciosa conocida e inteligencia de terceros para detectar con precisión las amenazas de API que se esconden a plena vista con tasas de alta eficacia líderes en la industria.
Cequence UAP permite a los clientes aprovechar continuamente las ventajas competitivas y comerciales de la conectividad API ubicua. La solución de Cequence da como resultado la futilidad, el fracaso y la fatiga de los ataques incluso para los atacantes más implacables. Mejora significativamente la visibilidad y la protección al tiempo que reduce los costos, minimiza el fraude, el abuso comercial, las pérdidas de datos y el incumplimiento. Obtenga más información en **www.cequence.ai**

Cequence: Protección continua para conectividad API ubicua