CEQUENCE

Ficha de dato

Descubrimiento de la superficie de ataque

Cequence API Spyder

A medida que las organizaciones evolucionan, sus redes cambian constantemente: se implementan nuevas aplicaciones, se actualizan las existentes y se incorporan nuevos proveedores de hosting por crecimiento orgánico o por fusiones y adquisiciones. Todas estas acciones fomentan la incorporación de nuevas APIs, ampliando una superficie de ataque ya de por sí extensa. La mayoría de las organizaciones simplemente no saben cuántas APIs tienen ni dónde se encuentran, y ese conocimiento es fundamental para cualquier programa de seguridad exitoso.

En cada organización, API Spyder descubre una media de:

326	197	37
Anfitriones API	**Dominios**	**Proveedores de alojamiento**

Esta superficie de ataque en continua expansión ha dado lugar a nuevos requisitos para los equipos de seguridad:

- Visibilidad y supervisión completas de las API públicas y los proveedores de alojamiento.
- Identificar posibles problemas de seguridad específicos de las API, como puntos finales OpenAPI o GraphQL expuestos públicamente.
- Informes personalizados sobre descubrimientos de superficies de ataque externas.

API Spyder de un vistazo

- **Descubrimiento de superficies de ataque externas,** incluidas API y proveedores de alojamiento
- **Algoritmos configurables por el usuario** para el descubrimiento y clasificación de APIs
- **Identificación de riesgos de API** con información procesable
- **Informes centrados en las personas** y exportación de datos detallados

Es fundamental tener visibilidad de las API de acceso público existentes, así como supervisar las nuevas API, especialmente las que pueden haberse hecho públicas accidentalmente, como los servidores que no están en producción o las aplicaciones en pruebas.

API Spyder Visión general

API Spyder es una herramienta de detección basada en SaaS que proporciona la visión de un atacante en los recursos de cara al público de una organización para encontrar hosts API externos e identificar proveedores de alojamiento no autorizados. Descubre metódicamente las API de cara al público y los proveedores de alojamiento, identifica problemas de seguridad específicos de las API y ofrece informes de nivel ejecutivo y de flujo de datos completo.

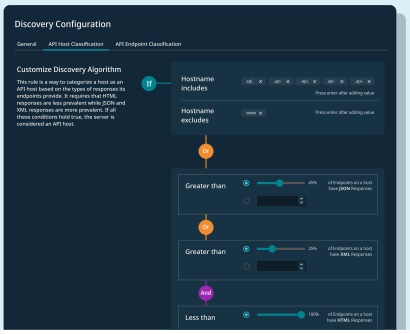
Características de API Spyder

Detección exhaustiva de la superficie de ataque externa

Sin instalación ni agentes en los endpoints, API Spyder realiza rastreos de descubrimiento basados en dominios o direcciones IP para identificar hosts de API y los proveedores de hosting asociados. Este método permite que API Spyder identifique hosts de API incluso si no están intercambiando datos, una capacidad crítica para encontrar hosts expuestos por accidente, como los mal configurados o remanentes de pruebas. Los rastreos pueden ejecutarse bajo demanda o programarse, y también pueden configurarse desde una geografía específica según se requiera por velocidad, geocercas (geo-fencing) o fines de privacidad de datos.

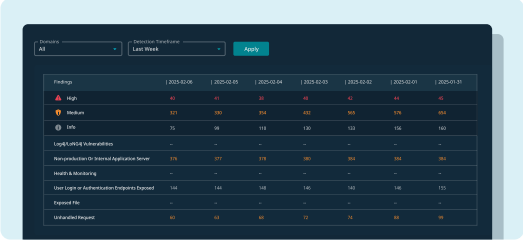
Algoritmos de descubrimiento y clasificación de API configurables por el usuario

Los recursos descubiertos por API Spyder se clasifican mediante algoritmos personalizables por el usuario. Cada organización y sector es diferente, y esta capacidad permite ajustar los algoritmos de descubrimiento y clasificación para alinearlos con el negocio y reducir falsos positivos. Por ejemplo, los usuarios pueden ajustar los algoritmos según el número o porcentaje de respuestas JSON, XML o HTML para mejorar la precisión de identificación de endpoints únicos o fuertemente modificados.



Identificación de riesgos de API

Durante el proceso de rastreo, API Spyder descubre hosts de API con problemas conocidos, incluidos endpoints Swagger, OpenAPI o GraphQL expuestos públicamente, o servidores de no producción. API Spyder categoriza estos hallazgos por función y severidad, con el contexto completo de la solicitud y la respuesta. Los hallazgos también son configurables por el usuario, lo que permite a las organizaciones enfocarse en los riesgos que consideren más relevantes.



Informes para ejecutivos y equipos de seguridad

API Spyder ofrece informes ejecutivos en PDF con visualizaciones para una vista de alto nivel. Los datos técnicos detallados pueden exportarse en formato Excel, incluyendo todos los hosts descubiertos por API Spyder, con detalles de cada host de API como dirección IP y hallazgos de seguridad.

Funciona con Cequence AI Gateway

Cequence AI Gateway habilita el acceso de IA agéntica (basada en agentes) a cualquier aplicación interna, externa o SaaS, en minutos y sin necesidad de código. API Security puede crear automáticamente especificaciones de API que el AI Gateway utiliza para crear servidores MCP, eliminando un esfuerzo manual significativo.

API Spyder forma parte de la plataforma Cequence Unified unificada de Cequence

La plataforma de Protección Unificada de API de Cequence une el descubrimiento, el cumplimiento y la protección a través de todas las API internas y externas para defenderse contra ataques, abusos dirigidos y fraude. API Spyder rastrea la superficie de ataque de las API externas, complementando el descubrimiento de API activas en API Sentinel. Cualquier problema descubierto puede mitigarse con API Spartan mediante el bloqueo nativo u otros métodos de mitigación. Las soluciones de Cequence se adaptan a las organizaciones gubernamentales, Fortune y Global 500 más exigentes, protegiendo más de 8.000 millones de llamadas API diarias y más de 3.000 millones de cuentas de usuario.

PLATAFORMA DE PROTECCIÓN API UNIFICADA

CEQUENCE
5201 Great America Pkwy, Suite 240, Santa Clara, CA 95054 | 1-650-437-6338 | info@cequence.ai | www.cequence.ai