CEQUENCE SECURITY

FICHA DE DATOS

Cequence API Spyder

Detección y administración continuas de la superficie de ataque de la API

Introducción

Hoy en día, casi todas las aplicaciones que usan sus empleados se basan en API. Las aplicaciones de productividad de ventas, colaboración, automatización de marketing y seguimiento de proyectos están basadas en API, al igual que todas las aplicaciones que pueden usar en su dispositivo móvil. A medida que las organizaciones continúen expandiendo su uso de microservicios y creen nuevas aplicaciones nativas de la nube, el uso de API seguirá aumentando, al igual que la superficie de ataque de API. Si no se documenta y prueba cuidadosamente, la superficie de ataque de su API puede incluir API de producción de acceso público, así como una gran cantidad de otros recursos y puntos finales que no deberían ser de acceso público. Los ejemplos incluyen servidores que no son de producción, especificaciones de API en desarrollo que incluyen un catálogo de puntos finales de servidores internos; puntos finales de monitoreo de salud que devuelven el estado del servidor de aplicaciones internas y mucho más.

- **Incapacidad para monitorear las API:**La falta de visibilidad implica falta de supervisión, lo que significa que la superficie de ataque de la API desconocida podría exponer a su organización a riesgos de seguridad, como filtraciones de datos, robo, fraude e interrupción del negocio.
- **Prueba incompleta:**Los esfuerzos de prueba de penetración o vulnerabilidad están incompletos porque no incluyen toda la superficie de ataque.
- **Auditorías fuera de cumplimiento:**La superficie de ataque desconocida plantea un desafío para los equipos de cumplimiento o auditoría que confían en conocer todas las formas en que se puede acceder a los datos corporativos.

Para abordar estos problemas, los equipos de seguridad deben poder descubrir toda su superficie de ataque de API y monitorearla constantemente en busca de nuevas API o dominios que se creen. También deben poder categorizar estas API según el riesgo e iniciar tareas de remediación para los equipos de seguridad y desarrollo.

API Spyder de un vistazo

No puede proteger ni administrar las API que no puede ver. API Spyder ayuda a los equipos de seguridad y cumplimiento de riesgos a descubrir su superficie de ataque de API expuesta públicamente, independientemente de dónde se implementen las API. Los beneficios clave incluyen:

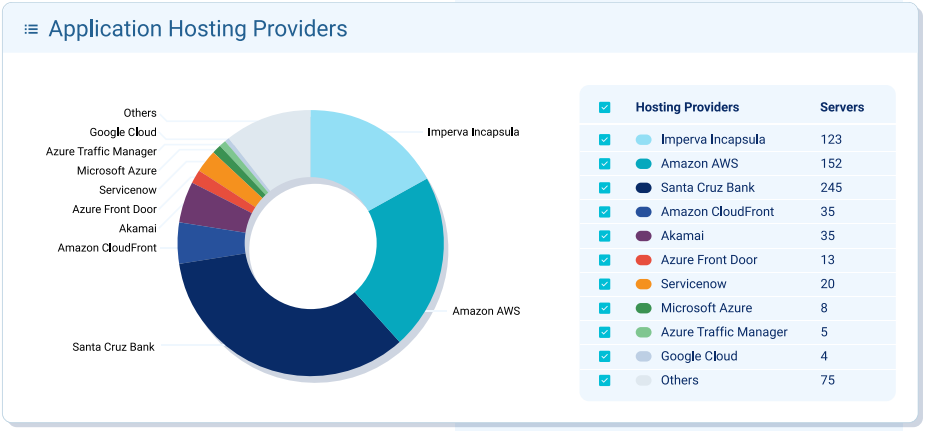
Visibilidad continuade API y puntos finales de producción y no producción expuestos públicamente ayuda a los equipos de seguridad a mantenerse al día con los esfuerzos de desarrollo de API.

Inventario actualizadode todas las implementaciones de proveedores de servicios en la nube y puertas de enlace que alojan API expuestas públicamente ayudan con las auditorías de riesgo y cumplimiento.

Informes exportablesy las notificaciones procesables en tiempo real de los recursos expuestos reducen los tiempos de respuesta de remediación del equipo de seguridad.

Visión general

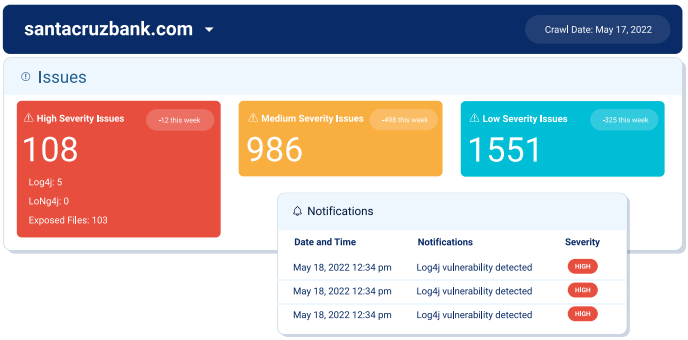
API Spyder adopta un enfoque único para descubrir la superficie de ataque de su API. Implementado completamente como un servicio en la nube y que no requiere la implementación de agentes o software, API Spyder rastrea de manera proactiva sus dominios para encontrar todos los subdominios de acceso público. Utiliza técnicas de sondeo patentadas para descubrir subdominios enumerados en DNS y sus puntos finales de API subyacentes. Una vez que se descubren los subdominios y los puntos finales de la API, API Spyder presenta los resultados en un panel fácil de usar que enumera todas las puertas de enlace de servicio que alojan las API y los tipos de puntos finales de la API descubiertos, clasificados por función. El tablero, los informes ejecutivos y las alertas en tiempo real le permiten traducir rápidamente los hallazgos en esfuerzos de remediación.



Funciones de API Spyder

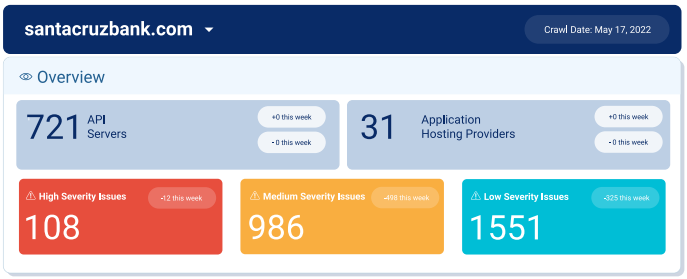
Descubra servidores vulnerables Log4j y LoNg4j

API Spyder se puede usar para validar que sus esfuerzos de parcheo de Log4j y LoNg4j estén completos y que no se hayan agregado servidores vulnerables adicionales a su cadena de suministro digital. Usando técnicas de rastreo predictivo, API Spyder descubre servidores públicos que aún no han sido parcheados para la vulnerabilidad Log4j y LoNg4j.



Descubra todos los proveedores de alojamiento de API

Al aceptar un dominio como entrada del usuario, API Spyder compila automáticamente un inventario de todos los subdominios de acceso público mediante técnicas de sondeo de DNS. Luego, API Spyder descubre automáticamente el servicio de alojamiento para cada subdominio, como una CDN o un proveedor de nube pública, y agrupa los subdominios por servicio de alojamiento para su revisión, análisis y reparación, si es necesario.



Descubra y categorice puntos finales de API de acceso público

Para eliminar la necesidad de especificaciones de API o catálogos como puntos de referencia, API Spyder utiliza una tecnología de rastreo predictivo patentada para descubrir los puntos finales de API expuestos públicamente para cada subdominio descubierto. Los endpoints descubiertos se clasifican por función (p. ej., autenticación), tipo de API (p. ej., REST o GraphQL), finalidad (p. ej., supervisión del estado o listas de Swagger) o audiencia prevista (p. ej., producción frente a no producción). También se clasifican en cada subdominio descubierto para que los equipos de seguridad los consuman fácilmente.

Notificaciones

API Spyder monitorea continuamente sus dominios, comparando los hallazgos anteriores con los resultados recién generados, y marca automáticamente cualquier cambio o desviación para tomar medidas. Los cambios en la superficie de ataque descubierta se visualizan mediante el tablero y se exportan como un archivo para compartir con otros usuarios para su reparación. Las notificaciones se generan por correo electrónico cuando se descubren nuevos servidores vulnerables Log4j/LoNg4j.

Informes accionables

Un informe ejecutivo predefinido resume los hallazgos por dominio, la cantidad de servidores API descubiertos y proveedores de alojamiento. Los hallazgos se clasifican aún más por niveles de riesgo y los proveedores de alojamiento se desglosan por tipo: ISP, infraestructura como servicio (IaaS) y CDN, lo que le permite descubrir posibles instancias de TI en la sombra. Para ayudarlo a realizar un seguimiento del progreso, el informe concluye con las diferencias de una semana a otra y un conjunto de acciones recomendadas.

API Spyder y la solución de protección de API unificada de Cequence

Un componente integral de la solución Cequence Unified API Protection, API Spyder complementa API Sentinel y Bot Defense con descubrimiento y monitoreo continuo de la superficie de ataque de API. Las organizaciones que han adoptado por completo una metodología API first o que recién están comenzando, confían en Cequence Security para proteger sus API y escalar su negocio con la única solución que aborda cada fase de su viaje de seguridad API. La solución Unified API Protection unifica la visibilidad de API en tiempo de ejecución, el monitoreo de riesgos de seguridad y la tecnología patentada de huellas dactilares de comportamiento para detectar y proteger constantemente contra ataques en línea en constante evolución. La solución ha demostrado ser eficaz en la prevención de fraudes en línea, ataques de lógica empresarial, exploits y fugas de datos no intencionadas.