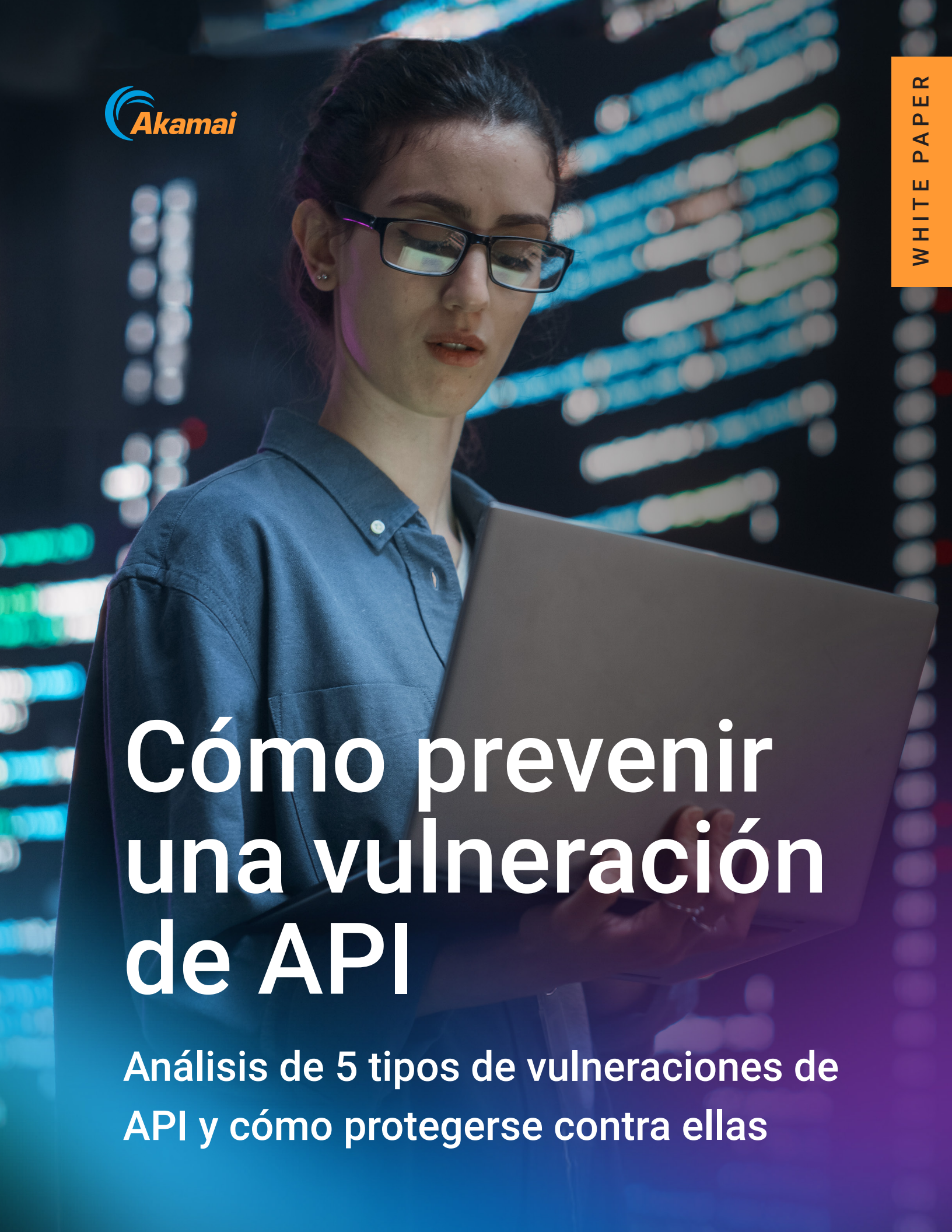


Akamai

WHITE PAPER

Cómo prevenir una vulneración de API

Análisis de 5 tipos de vulneraciones de API y cómo protegerse contra ellas

En este informe

Introducción

Las API conectan su empresa mediante el intercambio de datos con partners, proveedores y clientes. Sin embargo, la seguridad de API sigue siendo poco exhaustiva en la mayoría de las organizaciones. De hecho, las API vulnerables se han convertido en una debilidad objetivo para las empresas en los últimos años, y los atacantes hacen un uso indebido de ellas para acceder a datos confidenciales, venderlos a otros atacantes o publicarlos para que todo el mundo los vea. En 2024, las marcas globales de telecomunicaciones de consumo, informática empresarial y colaboración virtual vieron cómo las vulneraciones de API permitían publicar enormes cantidades de datos confidenciales de clientes y de otro tipo, lo que provocaba elevados costes financieros y de reputación.

¿Qué es una vulneración de API?

En pocas palabras, una vulneración de API es cualquier uso indebido o malintencionado de una API, a menudo para obtener acceso a datos confidenciales. Los tipos de vulneraciones de API se pueden subdividir según varios criterios. Para identificar los riesgos y evitar vulneraciones en las operaciones de producción, resulta útil considerar el siguiente esquema, que divide los riesgos en cinco categorías:

1. **Vulnerabilidades conocidas**
   - Los atacantes aprovechan las vulnerabilidades conocidas a las que aún no se han aplicado parches.
2. **API en la sombra, no aprobadas, zombis y obsoletas**
   - Las API no gestionadas y olvidadas pueden dejar las operaciones en una posición vulnerable.
3. **Exposiciones externas**
   - Puede que haya credenciales, claves y otras exposiciones fuera de su control.
4. **Errores de configuración y errores del operador**
   - Los errores de configuración de seguridad en la infraestructura y los servicios pueden crear puntos de entrada que los atacantes pueden explotar.
5. **Vulnerabilidades y errores no detectados**
   - Los atacantes buscan identificar los errores y las vulnerabilidades que han pasado al entorno de producción a pesar de sus esfuerzos para que esto no sucediera.

En este eBook se explica dónde se producen los fallos de seguridad en cada uno de estos cinco tipos de vulneraciones de API y cómo prevenirlas. Este eBook también tiene como objetivo ayudarle a identificar los puntos débiles específicos de su programa de seguridad de API para maximizar la seguridad al respecto y minimizar los riesgos.

Tipo de vulneración: vulnerabilidades conocidas

Las vulneraciones de API que aprovechan las vulnerabilidades conocidas (a las que aún no se han aplicado parches) son probablemente las más frecuentes. Si los ciberdelincuentes quieren obtener sus datos, un primer paso común es que comprueben si su organización ha dejado alguna puerta trasera abierta.

En enero de 2024, un atacante puso en peligro una herramienta de gestión de proyectos muy utilizada al atacar un terminal de API que carecía de controles de autenticación. Después de vulnerar la API, el atacante obtuvo acceso no autorizado a la información de millones de usuarios y, meses después, filtró más de 21 GB de datos en Internet, incluidas las direcciones de correo electrónico y los miembros de la junta.

Los problemas de autenticación y autorización se encuentran entre los problemas de API más comunes. Los 10 principales riesgos de seguridad de las API según OWASP proporcionan información sobre las 10 vulnerabilidades de API más importantes contra las que las organizaciones deben protegerse, incluida la autenticación comprometida.

Además de proteger las API de los tipos de riesgo incluidos en los 10 principales riesgos de seguridad según OWASP, las organizaciones deben proteger el código de API con respecto de la lista completa de vulnerabilidades y exposiciones comunes (CVE) creada por el centro de investigación y desarrollo financiado con fondos federales (FFRDC) en materia de ciberseguridad nacional de EE. UU., gestionado por la organización MITRE. Puede que recuerde la conocida vulnerabilidad Apache Log4j 2 (CVE-2021-44228), también conocida como "Log4Shell". Debido a un error en la biblioteca Log4j, una conocida biblioteca de registro de código abierto para el lenguaje de programación Java, los atacantes podían ejecutar código arbitrario de forma remota para obtener acceso al sistema. Los agentes maliciosos sondean periódicamente los sistemas empresariales en busca de vulnerabilidades conocidas como esta.

En Estados Unidos, la Agencia de Seguridad Cibernética y de la Infraestructura (CISA) mantiene un catálogo de CVE conocidas. Otros países pueden mantener catálogos similares.

La lista de los 10 principales riesgos de seguridad de las API según OWASP se creó en 2019 y se actualizó en 2023. Aunque es útil, no es capaz de seguir el ritmo de cambio en la superficie de ataque. Solo en 2024, se han añadido más de 24 000 nuevas CVE al catálogo de CISA, más de 500 de las cuales están relacionadas con las API (a fecha de mediados de agosto de 2024).

Para proteger completamente a su organización de las vulnerabilidades conocidas, es necesario realizar un esfuerzo en dos flancos:

1. Asegúrese de que sus procesos de desarrollo y pruebas son lo suficientemente sólidos como para evitar la introducción de vulnerabilidades conocidas en el entorno de producción.

2. Aplique parches a las nuevas vulnerabilidades lo antes posible una vez identificadas.

Muchas organizaciones tienen dificultades con estos dos pasos. Además, utilizan API y código de fuentes de terceros que pueden introducir toda otra serie de vulnerabilidades. En 2022, un equipo de investigadores descubrió fallos críticos de API que afectaban a varios fabricantes del sector de la automoción. Estos fallos podrían haber expuesto datos confidenciales de clientes e incluso la ubicación de un vehículo, lo que permitiría desbloquear, arrancar o desactivar un vehículo a través de un sistema de gestión remota comprometido.

Cómo prevenirlas

Una forma bien conocida de proteger a su organización frente a las vulneraciones de API debidas a vulnerabilidades conocidas es actualizar rápidamente el software y los sistemas cuando se publiquen parches de seguridad. También es esencial asegurarse de seguir unos procesos de desarrollo y pruebas exhaustivos y basados en las prácticas recomendadas de seguridad de API. Esto incluye:

- **Protección de la cadena de suministro de software:** asegúrese de que todas las bibliotecas, el software de código abierto (OSS) y cualquier otro código de terceros que utilice sean seguros.
- **Implementación de pruebas de seguridad "shift-left":** traslade las tareas relacionadas con la seguridad de API y las pruebas de software a las primeras etapas del proceso de desarrollo. Esto le puede ayudar a detectar vulnerabilidades, como errores en el código y de configuración, que los equipos de desarrollo puedan haber introducido por la presión de entregar rápidamente software o actualizaciones.
- **Aprovechamiento de la gestión de la estrategia de seguridad de API:** esto combina la detección de API con la identificación de datos confidenciales y la detección de vulnerabilidades, lo que garantiza que las medidas de corrección se centren primero en las API más críticas.

Cómo le ayuda Akamai API Security

Akamai API Security permite a sus equipos reducir las vulnerabilidades conocidas de cada nueva compilación sin sacrificar la velocidad. API Security es una solución de pruebas de seguridad de API diseñada específicamente que proporciona una cobertura completa de las vulnerabilidades específicas de API. Las pruebas activas ayudan a incorporar las pruebas de seguridad de API en todas las fases del desarrollo.

- **Detecte y pruebe cada API** basándose en la comprensión de la lógica empresarial de la aplicación.
- **Realice pruebas de seguridad "shift-left"** con integraciones en todo el ciclo de vida de desarrollo de software. Los equipos obtienen visibilidad dinámica de las API en varios estados y entornos a lo largo del proceso de integración e implementación continuas (CI/CD).
- **Proporcione a los desarrolladores** la mayor facilidad de uso, con una configuración y automatización sencillas, resultados de pruebas en línea y orientación contextual para la corrección de los problemas identificados.

Además, la gestión de la estrategia de API Security proporciona una visión completa del tráfico, el código y las configuraciones para evaluar el nivel de seguridad de sus API. API Security analiza el conjunto más amplio posible de fuentes para detectar vulnerabilidades, lo que incluye los archivos de registro, las repeticiones del tráfico histórico, los archivos de configuración y muchos otros elementos. También detecta todas las vulnerabilidades incluidas en la lista de los 10 principales riesgos de seguridad de las API según OWASP. Para obtener más información sobre la gestión de la estrategia, consulte la sección "Errores de configuración y errores del operador".

Tipo de vulneración: API en la sombra, no aprobadas, zombis y obsoletas

No puede proteger lo que no puede ver y, en muchas empresas, un gran porcentaje de API no están gestionadas, lo que hace que las API en la sombra, no aprobadas, zombis y obsoletas (consulte la barra lateral de la página siguiente) sean objetivos que no se ven o no se tienen en cuenta en su entorno de API. Además, los atacantes a menudo buscan variantes de API que pueden explotar: examinan las API expuestas de una organización y, a continuación, utilizan la técnica de fuzzing o modifican valores para encontrar versiones anteriores.

Esto es lo que sucedió con una gran empresa australiana de telecomunicaciones que accidentalmente expuso más de 11,2 millones de registros de clientes, incluidos los nombres, las direcciones, las fechas de nacimiento y algunos números de identificación emitidos por el gobierno. El ataque aprovechó una API utilizada para realizar pruebas que, de alguna manera, se había vuelto accesible a Internet. Dado que esta API no aprobada no tenía controles de autenticación, un atacante pudo solicitar y recibir millones de registros.

La mayoría de las organizaciones utilizan una amplia variedad de API heredadas y nuevas. Lamentablemente, es demasiado común encontrar junto a ellas API no aprobadas, zombis y en la sombra que exponen a la empresa a una serie de riesgos de ciberseguridad y dificultades operativas.

Estas API ocultas tienen una variedad de fuentes:

- **API comerciales:** algunos paquetes de software comercial incluyen API para crear conexiones con otras aplicaciones y fuentes de datos externas. Estas se pueden activar sin que nadie se dé cuenta (y es un problema que se puede solucionar mediante una detección exhaustiva de API).
- **Versiones anteriores de API:** en muchas ocasiones, puede que nunca se elimine una versión anterior de una API, a menudo con una seguridad más débil o una vulnerabilidad detectada. Es posible que una versión antigua deba coexistir con una nueva versión durante algún tiempo mientras se actualiza el software, pero cuando los fallos del proceso impiden que la API antigua se desconecte, se convierte en una API zombi.
- **Atajos y procesos que no se siguen:** las API en la sombra son el resultado de no informar a las personas adecuadas. Por ejemplo, es posible que el equipo de una línea de negocio cree API para dar respuesta a sus propias necesidades sin informar a los equipos de TI o de seguridad, o que un desarrollador no siga el procedimiento establecido.
- **API heredadas:** las API que se han "heredado" como parte de fusiones o adquisiciones también suelen pasar inadvertidas y se convierten en API en la sombra.
- **Código reactivado:** en algunos casos, las versiones antiguas de las API pueden reactivarse accidentalmente.

Cómo prevenirlas

Una auditoría manual para documentar y crear un inventario preciso de todas las API puede tardar horas, especialmente si se tiene en cuenta el tiempo que se tarda en evaluar y tomar medidas sobre cada API que se detecta. Esta no es una tarea realista para los equipos de seguridad que ya están sobrecargados de trabajo. Para proteger su empresa frente a la explotación de API no aprobadas, zombis y en la sombra, necesita un sistema de detección automatizado de API que sea capaz de identificar todas las API en uso y de todos los tipos. Es fundamental localizar y crear un inventario con todas las API de sus operaciones, así como detectar las API y los dominios de API que no están gestionados por una puerta de enlace de API.

Cómo le ayuda Akamai API Security

API Security aprovecha una amplia colección de fuentes de integración para la ingesta de datos de API, como el tráfico sin procesar, el registro y mucho más. Los datos derivados de estas fuentes permiten a API Security identificar las API, sus errores de configuración, sus vulnerabilidades y el uso indebido de las mismas. Nuestras herramientas detectan todas las vulnerabilidades incluidas en la lista de los 10 principales riesgos de seguridad de las API según OWASP.

Las capacidades de detección adicionales le permiten:

- Localizar y hacer inventario de todas sus API, independientemente de la configuración o el tipo, incluidas RESTful, GraphQL, SOAP, XML-RPC, JSON-RPC y gRPC.
- Detectar las API inactivas, heredadas y zombis.
- Identificar dominios ocultos olvidados, descuidados o desconocidos.
- Mantener los inventarios de API y garantizar la precisión de la documentación de API.

API no gestionadas de alto riesgo que buscan los atacantes

Las API en la sombra (también conocidas como "API no documentadas") existen y operan fuera de los canales supervisados oficiales de una organización. Puede que las hayan creado desarrolladores con buenas intenciones para acelerar su trabajo, o pueden ser un remanente de versiones de software anteriores.

Las API no aprobadas son API maliciosas o no autorizadas que suponen un riesgo para la seguridad de un sistema o una red.

Las API zombis incluyen cualquier API que permanezca en ejecución incluso después de que se haya sustituido por nuevas versiones u otras API por completo.

Las API obsoletas son API que ya no se recomiendan para su uso debido a cambios en las mismas. Aunque las clases, los métodos y los campos obsoletos sigan vigentes, puede que se eliminen en futuras implementaciones, por lo que no debe utilizarlos en código nuevo.

Tipo de vulneración: exposiciones externas

Las vulnerabilidades externas de las API suelen ser el resultado de prácticas deficientes o errores de procedimiento, como la filtración de credenciales y claves de API, la exposición del código y el esquema de API, las malas prácticas de documentación y las vulnerabilidades de los repositorios. La capacidad de detectar posibles vectores de ataque fuera de los límites de sus operaciones se ha convertido en un imperativo. En el último año, se han producido varias vulneraciones de gran repercusión debido a la exposición accidental de claves de API u otras credenciales a partir de fuentes externas. Por ejemplo, los hackers utilizaron una campaña de phishing para obtener acceso no autorizado a 130 de los repositorios de código fuente de Dropbox. Esto les permitió acceder a claves de API que estaban almacenadas de forma inadecuada en GitHub. Este tipo de exposición se ha vuelto tan común que GitHub ha tomado medidas para bloquear las filtraciones de claves de API y otros secretos, pero otros repositorios públicos pueden seguir siendo vulnerables.

En otro ejemplo de exposición externa con un gran seguimiento mediático, los investigadores descubrieron más de 3000 aplicaciones móviles que exponían claves de API de Twitter al público general. Este tipo de error es sorprendentemente común porque los desarrolladores a menudo incrustan claves de API en el código de la aplicación durante el desarrollo para una mayor comodidad. Si no eliminan las claves incrustadas antes del lanzamiento público, esta técnica puede convertirse en una fuente potencial de exposición de claves.

Cómo prevenirlas

Reducir o eliminar estos tipos de exposiciones externas requiere un ataque en dos flancos:

- Refuerce los procedimientos para identificar y eliminar las fuentes de exposición, como las claves y credenciales filtradas, el uso inadecuado de los repositorios, etc.
- Analice periódicamente la superficie de ataque externa para detectar y corregir vulnerabilidades.

Para protegerse frente a la gama más amplia de amenazas de API, necesita tanto la detección de dentro hacia fuera (como se describe en la sección sobre las vulnerabilidades de API no aprobadas) como la detección de fuera hacia dentro, que puede identificar exposiciones y reducir su superficie de ataque externa.

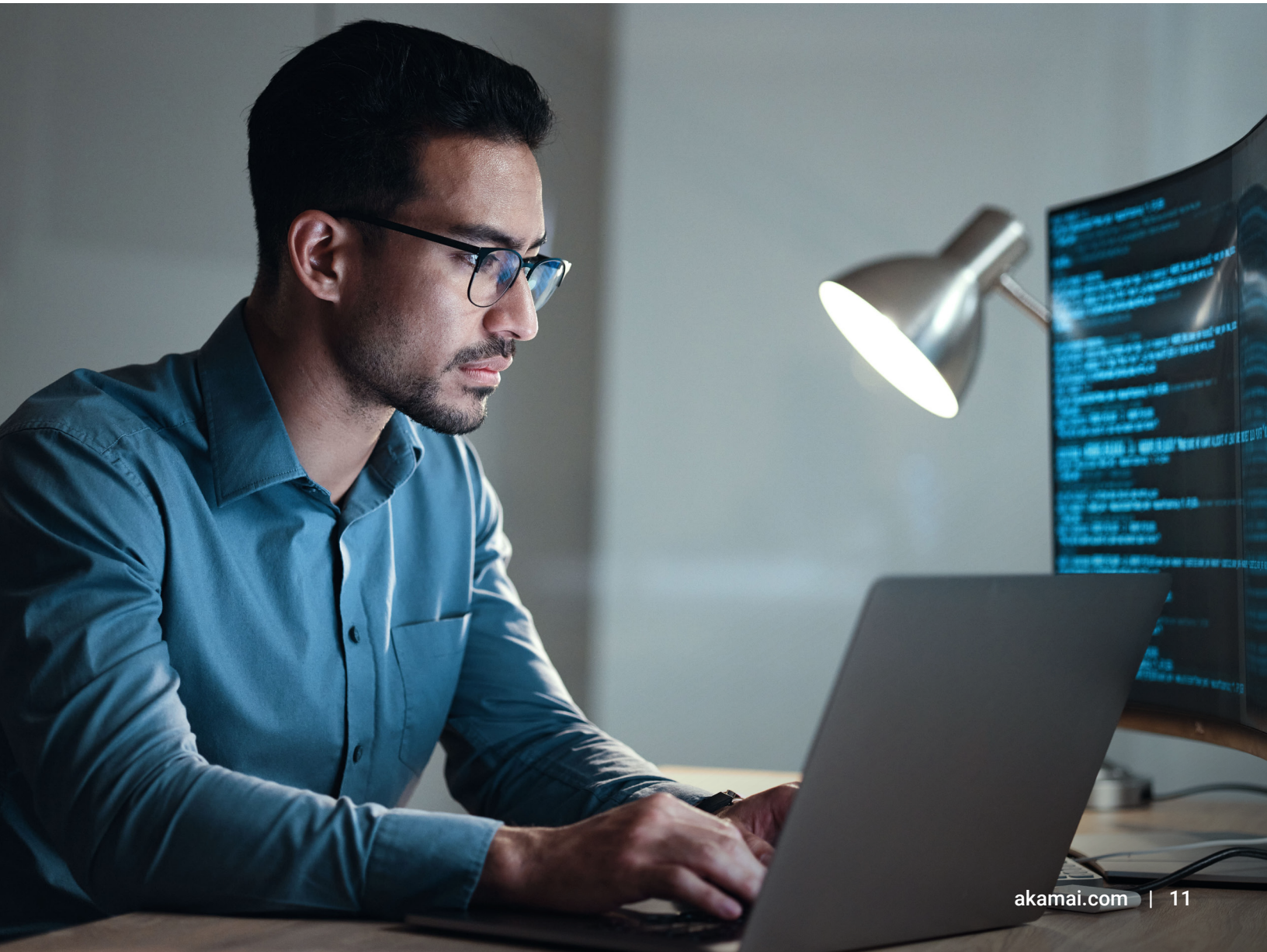
Cómo le ayuda Akamai API Security

API Security le ayuda a adelantarse a los atacantes mediante la simulación de las técnicas de reconocimiento que utilizan los hackers y al permitirle detectar y corregir los problemas rápidamente. Con la detección de fuera hacia dentro, API Security analiza automáticamente su superficie de ataque externa a intervalos regulares para detectar las vulnerabilidades antes que los atacantes, lo que le permite:

- **Descubrir vulnerabilidades públicas:** encuentre y corrija rápidamente problemas críticos como filtraciones de credenciales y claves de API, exposición de código, errores de configuración, vulnerabilidades de los repositorios y mucho más.
- **Detectar dominios y subdominios relacionados con su empresa:** aproveche los datos recopilados de varias fuentes, incluidos registradores de Internet, registradores de certificados y código abierto.
- **Incorporar métodos de ataque reales:** simule que un atacante realiza un reconocimiento externo para recopilar información mediante la ejecución de consultas limitadas a los dominios o subdominios de la empresa.

Tipo de vulneración: errores de configuración y errores del operador

Muchos ciberatacantes obtienen acceso explotando los errores de configuración de los servidores, las redes, las puertas de enlace de API y los firewalls que actúan como intermediarios y protegen el tráfico de las API. Un estudio de IBM Security X-Force reveló que dos tercios de las vulneraciones en la nube están vinculadas a API que presentan errores de configuración. Los errores de configuración de seguridad pueden deberse a configuraciones predeterminadas inseguras, almacenamiento en la nube sin control de acceso (sorprendentemente común) y configuraciones incompletas o ad hoc. A medida que su huella digital se amplía, sus operaciones pueden ampliarse a más ubicaciones, incluidas varias zonas de disponibilidad de nube pública o nubes públicas como AWS, Microsoft Azure y Google Cloud. Estos entornos a menudo utilizan controles de seguridad diferentes, por lo que garantizar una configuración correcta de la seguridad en todos ellos es una tarea difícil y compleja.



Cómo prevenirlas

Una de las mejores formas de protegerse contra los errores de configuración de seguridad en el lado de la infraestructura es evitar en la medida de lo posible la configuración manual de servidores, dispositivos de red, puertas de enlace y firewalls. Si los equipos de administración de su empresa configuran habitualmente los controles de seguridad de la infraestructura y las aplicaciones de forma manual, o los "ajustan" periódicamente, la posibilidad de introducir vulnerabilidades de configuración aumenta.

Cuando se trata de la seguridad, la automatización es su mejor aliado. Algunas empresas están adoptando la idea de una infraestructura inmutable como una forma de evitar los errores manuales.

Incluso cuando haya hecho todo lo posible para garantizar que su infraestructura, sus servicios y sus API sean infranqueables, seguirá necesitando una herramienta de gestión de la estrategia de API. La gestión de la estrategia le proporciona las herramientas necesarias para gestionar, supervisar y mantener la seguridad durante todo el ciclo de vida de las API.

Cómo le ayuda API Security

El módulo de gestión de la estrategia de API Security analiza las llamadas y la infraestructura de API para identificar los posibles errores de configuración. Estos errores suelen deberse a problemas de categoría de Amazon S3, datos confidenciales en API no autenticadas y distintos errores de configuración basados en el acceso de Kubernetes.

El módulo de gestión de la estrategia proporciona una visión completa del tráfico, el código y las configuraciones, lo que permite ver toda la superficie de ataque en las API y las aplicaciones web, incluidos todos los tipos de datos confidenciales que se transfieren a través de las API, como la información de identificación personal. También le ayuda a confirmar que su herramienta de gestión de API utiliza protocolos y cifrados sólidos para evitar la posible exposición de estos datos confidenciales. Además, las API no deben aceptar tokens web JSON caducados, ya que esto permitiría el acceso no autorizado y aumentaría los riesgos de seguridad. El módulo también ayuda a evitar errores de configuración, como balanceadores de carga de aplicaciones que escuchan en puertos no seguros sin redirección. Todas estas medidas refuerzan colectivamente la estrategia de seguridad de las API, lo que garantiza una defensa más resiliente frente a posibles amenazas.

Tipo de vulneración: vulnerabilidades no detectadas

Al igual que con la mayoría de los tipos de vulneraciones, los ciberdelincuentes que analizan su infraestructura suelen buscar CVE, los 10 principales riesgos de seguridad según OWASP y otros errores de configuración comunes, así como API no aprobadas, zombis y en la sombra. También sondean las API expuestas en busca de nuevas vulnerabilidades que pueden explotar en bibliotecas, código abierto y otros tipos de código público, así como en errores de codificación y configuración u otros errores, en su entorno de API. Estas vulnerabilidades permiten a los ciberdelincuentes manipular las llamadas a las API e insertar cadenas de fuzzing en las solicitudes. Como resultado, las técnicas que utilizan los ciberdelincuentes evolucionan constantemente.

Cómo prevenirlas

Una parte importante de la prevención consiste en garantizar que el código esté lo más libre posible de errores y vulnerabilidades (consulte la sección "Vulnerabilidades conocidas"). Sin embargo, debe asumir de todas formas que los atacantes encontrarán errores u obtendrán acceso a claves o credenciales que les permitan explotar las API.

La protección en tiempo de ejecución de API está diseñada para identificar a los hackers que explotan cualquier vulnerabilidad, ya sea conocida o desconocida. Es la única forma de proteger su entorno de API contra errores de configuración y otros errores que no han sido identificados previamente, y que se introducen en el entorno de producción, y es la mejor protección contra credenciales y claves que se han visto comprometidas.

La protección en tiempo de ejecución identifica patrones y anomalías inusuales en el uso de las API y el acceso a los datos, de modo que los ataques en curso que podrían pasar desapercibidos se puedan identificar y corregir antes de que se extraigan miles o millones de registros de datos.

La protección en tiempo de ejecución de API le ayuda a identificar y bloquear solicitudes de API maliciosas, incluidos:

- Ataques que extraen grandes volúmenes de datos confidenciales de una API
- Ataques de autorización a nivel de objeto comprometida (BOLA)

Una solución de protección en tiempo de ejecución de API puede detectar:

- Filtración de datos
- Infracciones de la política de datos
- Ataques contra la seguridad de API
- Manipulación de datos
- Comportamiento sospechoso

Además, esta protección en tiempo de ejecución debe registrar el tráfico de las API, supervisar el acceso a datos confidenciales, detectar amenazas y bloquear o corregir vectores de ataque.

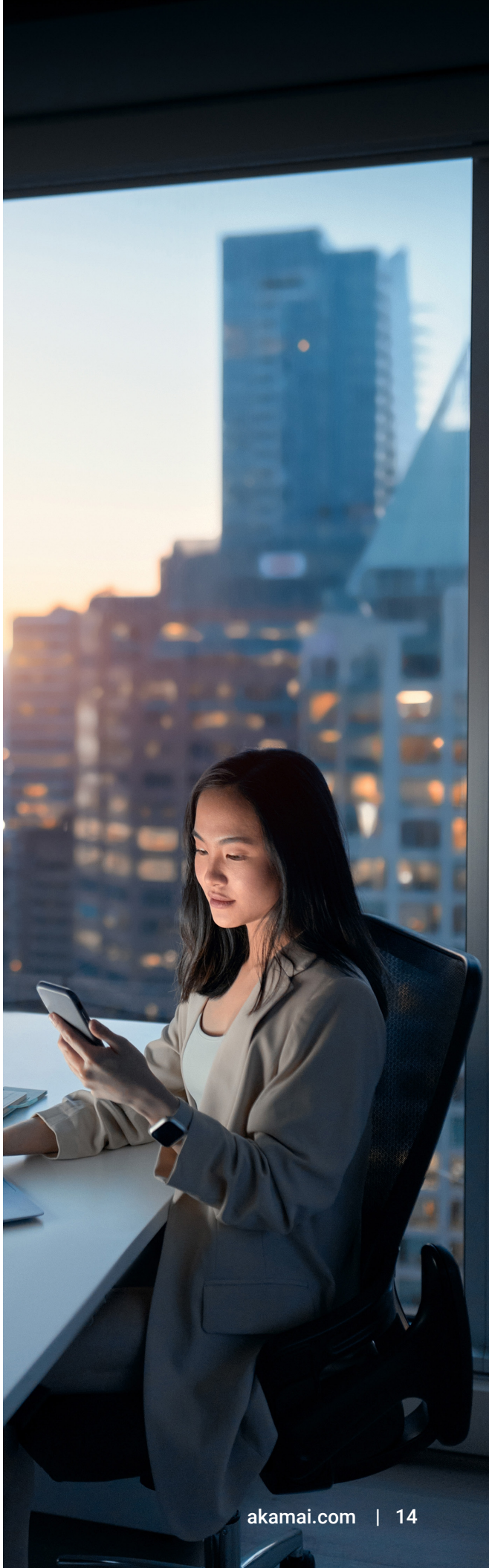
Cómo le ayuda API Security

Piense en la protección en tiempo de ejecución como su última línea de defensa cuando otras medidas de prevención se quedan cortas. La función principal de la protección en tiempo de ejecución es detectar y bloquear los ataques a la API en tiempo real. La supervisión autónoma basada en el aprendizaje automático (ML) se utiliza para realizar análisis del tráfico en tiempo real y proporcionar información contextual sobre la filtración de datos, la manipulación de datos, las infracciones de políticas de datos, los comportamientos sospechosos y los ataques a la seguridad de API. API Security detecta anomalías y posibles amenazas en su tráfico de API, y facilita la corrección en función de políticas de respuesta a incidentes preseleccionadas.

Mediante el aprendizaje automático, API Security crea un modelo de comportamiento para cada API. Esta línea de base del comportamiento normal se utiliza para detectar ataques a la lógica empresarial de API. Cada problema generado por la protección en tiempo de ejecución incluye la gravedad, el estado, una asignación a los 10 principales riesgos de seguridad de las API según OWASP y detalles del atacante, cuando corresponda. Los problemas también incluyen pruebas, como los detalles de la sesión del atacante y una copia de la solicitud y respuesta de la API, para ayudar a clasificar y corregir el problema.

La protección en tiempo de ejecución de API Security ofrece detección y prevención en tiempo real de ataques de API junto con detección continua de errores de configuración de API, además de muchas integraciones de flujos de trabajo populares que simplifican las operaciones y la corrección.

Quizás la mejor noticia para su equipo sea que API Security se integra con WAF, puertas de enlace de API, ITSM, SIEM y otras herramientas de flujo de trabajo para ofrecer una defensa holística contra los ataques. Puede optar por automatizar completamente la corrección de amenazas o requerir diferentes niveles de intervención manual para obtener una mayor visibilidad y control.



5 tipos de vulneraciones, 5 principios de prevención

Ahora que comprende mejor cómo utilizan los ciberdelincuentes las API, puede centrarse en protegerlas. A continuación se muestran las cinco herramientas de prevención y las perspectivas estratégicas que debe utilizar de forma conjunta:

1. Seguridad de API con enfoque "shift-left"

- La seguridad de API con enfoque "shift-left" significa probar ampliamente las API en el entorno de desarrollo para no exponer vulnerabilidades en su entorno de producción, en el que los ciberdelincuentes pueden encontrarlas.

2. Detección de dentro hacia fuera

- Identifique todas las API que existen en su entorno.

3. Detección de fuera hacia dentro

- Identifique y elimine las fuentes de exposición, como las claves y credenciales filtradas, y el uso inadecuado de los repositorios, y analice periódicamente la superficie de ataque externa para detectar y corregir vulnerabilidades.

4. Gestión integral de la estrategia

- Avance siempre con buen pie en lo que respecta a la seguridad de API evitando errores de configuración y vulnerabilidades.

5. Protección en tiempo de ejecución

- Detecte la actividad anómala de las API y protéjase contra todas las amenazas posibles, incluidos los errores y vulnerabilidades que no han sido identificados previamente.

Solicite una demostración

Vea Akamai API Security en acción y descubra lo fácil que es identificar y solucionar errores de configuración en sus API, y protegerse de ataques maliciosos a las API. Descubra de primera mano por qué las principales empresas eligen nuestra solución de seguridad de API.

Obtener una demostración