Guía del comprador de seguridad de las API

Superar el reto de seguridad de las API

A medida que las organizaciones se digitalizan y centran cada vez más en la nube, sus API crecen en alcance y escala, lo que las hace más valiosas. En la actualidad, las API:

- Son la base de las aplicaciones y los servicios que se utilizan para prestar servicios a los clientes y partners, lo que incluye las últimas innovaciones de IA.
- Están integradas en los entornos de nube, desde los servicios que utilizan los desarrolladores hasta las cargas de trabajo que migran los ingenieros.
- Son fuentes de ingresos en sí mismas, ya que ayudan a ampliar el negocio y crear un ecosistema de desarrolladores.

Sin embargo, si su caso es como el del 78 % de los profesionales de TI y seguridad que han experimentado incidentes de seguridad de las API[1], también habrá experimentado de primera mano que las API son un riesgo cada vez mayor. Las API expuestas o mal configuradas prevalecen, están desprotegidas y son fáciles de vulnerar. A menudo, muchas organizaciones ni siquiera saben cuántas API tienen y no pueden gestionarlas todas. Estas API inactivas, o zombis, son vectores de ataque clave.

Hay mucho en juego. Los ataques a sus API pueden poner en peligro los ingresos, la resiliencia y el cumplimiento normativo de una empresa. La mayoría de las organizaciones aún no cuentan con los controles y las capacidades adecuados para evitar los ataques a las API. Es cierto que muchas empresas tienen herramientas de API en su pila actual, lo que incluye puertas de enlace de API y firewalls de aplicaciones web. Sin embargo, aunque estas herramientas pueden ofrecer cierta protección, no se han diseñado para proporcionar el grado de visibilidad, seguridad en tiempo real y pruebas continuas que hacen falta para defenderse de los ataques a API modernos.

1. Akamai Technologies, “API Security Disconnect Report,” 2023

Entonces, ¿qué se necesita para proteger todo el entorno de API? Aunque en los últimos años han surgido muchos productos de seguridad de las API, puede ser complicado elegir una solución entre tantos proveedores y capacidades.

Las amenazas actuales exigen una solución completa de seguridad de las API que abarque cuatro áreas críticas: detección, gestión de la estrategia, detección y corrección de amenazas y pruebas de seguridad de API. En esta guía del comprador se describen las capacidades clave que debe tener una solución completa de seguridad de las API, para lo que se definen las funciones y los controles de seguridad necesarios para desarrollar y mantener API seguras al tiempo que se localiza y protege cada API del ecosistema.

Capacidades clave para proteger de forma exhaustiva las API

Para determinar las capacidades de seguridad de las API que necesita, es importante comprender la naturaleza de los retos a los que se enfrenta.

Las API suelen estar repartidas por varios entornos, que pueden ser desde locales hasta de nube híbrida. Y, por si la situación no fuese lo bastante compleja, es probable que su ecosistema de API vaya más allá de su propia red y presencia en la nube. Piense en la infinidad de conexiones que han establecido sus API con aplicaciones, servicios y sistemas de terceros, que pueden o no priorizar la seguridad de las API.

Además, es difícil obtener información en tiempo real sobre:

- Dónde se enrutan las API
- Cómo se configuran
- Qué datos confidenciales mueven
- Qué riesgos representan

A medida que las empresas aceleran el desarrollo y la implementación de nuevas aplicaciones y API, la superficie de ataque crece exponencialmente. En lo que respecta a las API anteriores, es posible que su organización diseñara y produjera una serie de API hace años, antes de que la seguridad de las API se convirtiera en una necesidad fundamental.

La falta de visibilidad tiene unas consecuencias preocupantes: solo 4 de cada 10 profesionales de seguridad con inventarios de API completos saben cuáles de sus API devuelven datos confidenciales cuando reciben una llamada. Muchas de estas llamadas a las API proceden de agentes maliciosos en busca de vulnerabilidades y, en cuanto detectan una brecha, los ataques suelen ser implacables.

A la hora de evaluar a los proveedores de seguridad que afirman que pueden proteger completamente sus API, es importante asegurarse de que cuentan con capacidades y controles en producción consolidados para las cuatro áreas críticas.

Si sigue leyendo, encontrará una serie de listas de comprobación del comprador que puede utilizar para evaluar las capacidades de los proveedores.

01

Detección de las API

Es habitual tener API que nadie conoce. Sin embargo, sin un inventario preciso, su empresa se expone a muchos riesgos. Para crear un inventario adecuado de sus API, debe poder:

- ☑ Localizar y realizar un inventario de sus API, independientemente de cuál sea su configuración o tipo.
- ☑ Detectar las API inactivas, heredadas y zombis.
- ☑ Identificar dominios ocultos olvidados, descuidados o desconocidos.
- ☑ Eliminar los puntos ciegos y descubrir posibles rutas de ataque.

02

Gestión de la estrategia de las API

Hasta los errores más básicos de configuración de API pueden abrir la puerta a los atacantes. Y una vez dentro, accederán y exfiltrarán rápidamente sus datos confidenciales. Para conocer la configuración de todas sus API, debe poder:

- ☑ Analizar automáticamente la infraestructura para detectar errores de configuración y riesgos ocultos.
- ☑ Crear flujos de trabajo personalizados para informar acerca de las vulnerabilidades a las principales personas afectadas.
- ☑ Identificar qué API y usuarios internos pueden acceder a los datos confidenciales.
- ☑ Clasificar los problemas detectados en función de la gravedad para priorizar la reparación de los más críticos.

03

Detección y corrección de amenazas de API

Los ataques a las API están volviéndose prácticamente inevitables. Para detectar y corregir con éxito las amenazas, debe poder:

- ☑ Supervisar la manipulación y filtración de datos, las infracciones de políticas, el comportamiento sospechoso y el uso indebido de las API.
- ☑ Analizar el tráfico de API de todas las fuentes e integrarlo con los flujos de trabajo existentes (incidencias, gestión de información y eventos de seguridad, etc.) para alertar a los equipos de operaciones y seguridad.
- ☑ Evitar los ataques y el uso indebido en tiempo real con correcciones parcial o totalmente automatizadas.

04

Pruebas de seguridad de las API

La velocidad es esencial a la hora de desarrollar aplicaciones, pero un ritmo de trabajo demasiado acelerado puede propiciar que no se detecten vulnerabilidades o defectos de diseño. Para probar correctamente sus API, debe poder:

- ☑ Realizar una amplia variedad de pruebas automatizadas que simulen el tráfico malicioso y sigan la lógica empresarial subyacente de las API.
- ☑ Detectar las vulnerabilidades antes de poner las API en funcionamiento para reducir el riesgo de que los ataques logren su objetivo.
- ☑ Analizar las especificaciones de sus API con respecto a las políticas y normativas de control establecidas.
- ☑ Realizar pruebas de seguridad bajo demanda dirigidas a las API o como parte de un proceso de integración e implementación continuas (CI/CD).

Detección de API: análisis detallado de las capacidades clave

Muchas organizaciones utilizan API tanto heredadas como nuevas. No es raro encontrarse con API no gestionadas en el entorno de producción de las que nadie de los equipos de operaciones y seguridad está al tanto, lo que expone a la empresa a todo tipo de riesgos de ciberseguridad y problemas operativos. Las API no autorizadas pueden surgir debido a factores como tomar atajos, no seguir adecuadamente los procesos o no desactivar una API cuando se ordena su retirada. En la página siguiente, ofrecemos una serie de ejemplos destacados que tener en cuenta.

API comerciales

Algunos paquetes de software comercial incluyen API para crear conexiones con otras aplicaciones y fuentes de datos externas. Es posible que estas API se activen sin que nadie se dé cuenta.

API que no se desactivan

También es posible que las API se retiren oficialmente, pero permanezcan en funcionamiento debido a descuidos operativos. Cuando se da esta situación es común hablar de "API zombis".

Versiones anteriores de API

A veces, una versión anterior de una API nunca se retira. Es posible que una versión anterior tenga que coexistir con una nueva versión durante un tiempo mientras se actualiza el software. Pero, ¿y si la persona responsable de desactivar la API deja la empresa, cambia de puesto o simplemente se olvida de desactivar la versión anterior?

Atajos y procesos que no se siguen

Algunas API no autorizadas son el resultado de no informar a las personas adecuadas. Por ejemplo, es posible que un equipo de línea de negocio (LOB) cree API para abordar sus propias necesidades sin informar al departamento de TI, o que a los desarrolladores les preocupe más la ejecución que los procedimientos. También es habitual pasar por alto API que se han "heredado" como parte de una adquisición. Estos tipos de API no autorizadas se conocen comúnmente como API en la sombra.

Cuando hable con los proveedores, pídales que le expliquen cómo se aseguran de identificar las API no autorizadas, heredadas, zombis y en la sombra y de encargarse de ellas antes de que los agentes maliciosos las pongan en el punto de mira. Las API heredadas y zombis suelen ser el eslabón más débil de las estrategias de seguridad de las API. Por tanto, es fundamental detectar API que no estén gestionadas por una puerta de enlace de API y localizarlas, realizar un inventario de ellas y determinar si requieren correcciones o hay que retirarlas.

Funciones clave de detección de API

Una solución de seguridad de las API debe contar con las siguientes funciones de detección

Detección e inventario detallado de activos de API

Una herramienta de detección de API debe poder localizar e identificar las API que tiene, independientemente de su tipo o configuración, lo que abarca RESTful, GraphQL, SOAP, XML-RPC, JSON-RPC y gRPC. También debe crear un inventario que se actualice automáticamente para evitar que quede obsoleto, así como proporcionar la capacidad de buscar, etiquetar, filtrar, asignar y exportar API en función de cualquier atributo.

Detección de las API inactivas, heredadas y zombis

Las API heredadas y zombis pueden ser anteriores a las iniciativas de seguridad de las API de su organización. Lo normal es que estas API no tengan dueño, no haya visibilidad de ellas y no se les apliquen controles de seguridad. Es fundamental que una herramienta de detección de API pueda localizar estas API.

Detección de dominios en la sombra

Además de API en la sombra, es posible que tenga dominios enteros en la sombra; es decir, nombres de dominio de API de los que no sabe nada. Las herramientas de detección de API deben poder identificar dominios en la sombra olvidados, descuidados o desconocidos que puedan suponer un riesgo para la seguridad.

Análisis automáticos

Los análisis son esenciales para eliminar los puntos ciegos e identificar problemas críticos, como:

- Claves y credenciales de API filtradas
- Exposición de esquemas y código de API
- Errores de configuración de la infraestructura
- Vulnerabilidades en páginas de documentación, repositorios de GitHub, espacios de trabajo Postman, etc.

Identificar estas y otras fuentes de inteligencia explotable también puede ayudar a los equipos a conocer las posibles rutas de ataque que podrían utilizar los ciberdelincuentes.

Desarrollo personalizado limitado

Finalmente, con la herramienta de detección de API adecuada, no debería necesitar desarrollo personalizado para sus fuentes de tráfico. Estas herramientas deben incluir integraciones predefinidas para los principales componentes de la infraestructura. El desarrollo personalizado suele llevar mucho tiempo y, si se producen cambios en el origen de la fuente, es probable que sea necesario modificar una integración, una tarea que los desbordados equipos de seguridad de TI no pueden escalar.

Gestión de la estrategia de las API: análisis detallado de las capacidades clave

Las amenazas a su entorno de API están creciendo rápidamente debido a tendencias como el paso de equipos de TI centralizados a operaciones de línea de negocio descentralizadas, el mayor uso de recursos en la nube y la transición a arquitecturas basadas en microservicios.

Una detección sólida (tal y como se describe en la sección anterior) es el primer paso para proteger su entorno de API. Debe poder detectar las API de todos los tipos que se utilizan actualmente y realizar un inventario de ellas.

Hay una serie de capacidades adicionales que son esenciales para gestionar su estrategia de seguridad para todas sus API. Debe poder identificar qué API acceden a datos confidenciales y transfieren datos de ese tipo para poder clasificarlas en consecuencia, ya que es imperativo que las API que manejan datos como información sobre los clientes cuenten con procesos de autenticación. También es importante identificar vulnerabilidades de la infraestructura que harán que cualquier API sea más vulnerable.

Evaluación de la configuración

Muchos ciberataques tienen éxito debido a un simple error de configuración de las redes, las puertas de enlace de API o los firewalls que actúan como intermediarios y protegen el tráfico de las API.

Una solución de seguridad de las API debe analizar con regularidad la configuración de la infraestructura y el software, lo que incluye los archivos de registro, las repeticiones del tráfico histórico, los archivos de configuración y muchos otros elementos. De esta forma, podrá detectar errores de configuración y vulnerabilidades, además de eliminar el riesgo de desviaciones de configuración.

Gravedad personalizable

A medida que la solución identifica nuevas vulnerabilidades en su entorno, también debe asignar un nivel de gravedad a los problemas detectados para poder priorizar su corrección. Los niveles de gravedad deben ser personalizables para que se ajusten a la tolerancia al riesgo, los requisitos normativos y las políticas internas de su organización.

Flujos de trabajo personalizados

Además de poder personalizar la gravedad, la herramienta ideal de gestión de la estrategia debería permitirle crear flujos de trabajo personalizados para tomar medidas de inmediato cuando se identifiquen vulnerabilidades. Estos flujos de trabajo pueden abarcar desde crear incidencias hasta notificar a los principales interesados o actualizar la configuración de red.

Documentación generada automáticamente

La documentación de las API indica a los usuarios para qué sirven las API y cómo utilizarlas. Las organizaciones deben asegurarse de que las API cumplan las especificaciones y dispongan de una documentación precisa. Una documentación deficiente o inexistente dificulta las pruebas de seguridad, lo que aumenta el riesgo de que una API llegue a producción sin que se detecte una vulnerabilidad. Este problema se ve agravado a menudo por la externalización del desarrollo de las API. Independientemente de la raíz del problema, la documentación desactualizada, incompleta e inexistente es inaceptable si desea que su programa de seguridad de las API tenga éxito.

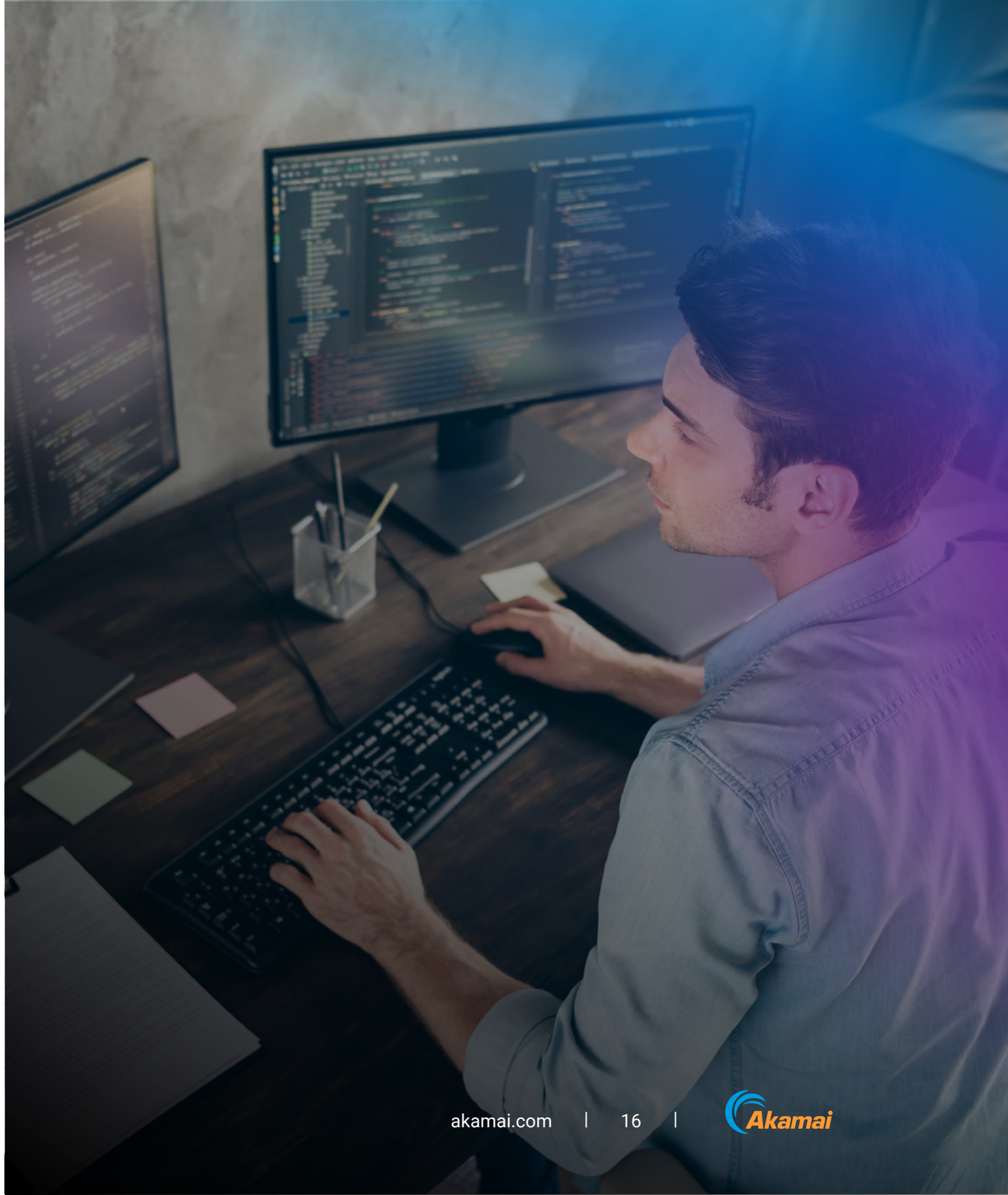
La especificación OpenAPI define descripciones de interfaces estándar. Una solución de seguridad de las API debe poder:

- Comparar las especificaciones de las API con tráfico observable real e identificar las diferencias, de modo que las organizaciones puedan ver cuáles de sus API implementadas no cumplen las especificaciones y pueden suponer un riesgo.
- Generar automáticamente documentación completa de OpenAPI basada en el estado actual y futuro de las API para ayudar a garantizar que todas las API estén debidamente documentadas y que la documentación esté actualizada. Identificar estas y otras fuentes de inteligencia explotable también puede ayudar a los equipos a conocer las posibles rutas de ataque que podrían utilizar los ciberdelincuentes.

Detección y corrección de amenazas de API: análisis detallado de las capacidades clave

Los ataques que intentan explotar las vulnerabilidades de las API ya son una realidad. Ya no se trata de si su organización será atacada, sino de cuándo y cómo. Se ha vuelto imperativo detectar rápidamente los ataques y bloquearlos antes de que puedan causar daños importantes, como la exfiltración de datos privados de clientes. Incluso si sus API son lo más seguras posible, necesita una protección activa del tiempo de ejecución para detectar casos de filtración y manipulación de datos, infracciones de políticas de datos, comportamientos sospechosos y ataques a la seguridad de las API. Esta protección debe registrar el tráfico de las API, supervisar el acceso a datos confidenciales, detectar amenazas y bloquear o corregir vectores de ataque, entre otras medidas.

En las dos páginas siguientes, explicamos las funciones más importantes que debe incluir una solución de seguridad de las API.



Supervisión fuera de banda en tiempo real

La supervisión de la seguridad de las API no debería afectar al tráfico de las API ni ralentizarlo. Busque proveedores que puedan ofrecer un enfoque sin agentes que permita a las empresas acelerar las implementaciones y ver más tráfico. No obstante, en circunstancias en las que sea pertinente (por ejemplo, en entornos locales complejos), la solución debe tener suficiente flexibilidad para admitir también el uso de agentes.

Una solución de seguridad de las API debe reflejar el tráfico de las fuentes de datos identificadas y realizar un análisis de esos datos de tráfico en segundo plano, con alertas en tiempo real de cualquier problema detectado.

Detección de anomalías y explotación de API

La recopilación pasiva de datos no es suficiente, especialmente teniendo en cuenta que el número de API y el volumen total de tráfico de las API siguen aumentando. La actividad de las API se debe analizar continuamente para detectar eventos anómalos y alertar a los equipos de seguridad y operaciones.

Las herramientas avanzadas incorporan tecnología de IA y aprendizaje automático para analizar el tráfico en tiempo real y emplear la información contextual para identificar actividades anómalas que puedan indicar casos de filtración y manipulación de datos, infracciones de políticas de datos y otros ataques a la seguridad de las API.

Prevención de ataques a las API

Cuando se identifica una anomalía u otro problema y se genera una alerta, el tiempo es esencial. Se debe detectar y bloquear el movimiento no autorizado de datos confidenciales a través de API u otro uso indebido sospechoso de las API. Una solución de seguridad de las API no solo debe bloquear el uso indebido mediante la integración con los firewalls y las puertas de enlace de API existentes, sino que también debe automatizar parcial o totalmente la corrección. Deben poder aplicarse correcciones semiautomatizadas para abordar algunos tipos de alertas. Para problemas recurrentes identificados previamente, debe tener la opción de proporcionar una respuesta totalmente automatizada.

Puntuación de confianza para los ataques

Algunas soluciones del mercado utilizan algoritmos de aprendizaje automático entrenados para evaluar señales externas e internas, como el comportamiento de las API, los patrones de tráfico de red, los datos de geolocalización y las fuentes de información sobre amenazas. Gracias a factores contextuales como estos, una solución puede determinar el nivel de confianza en que un incidente durante el tiempo de ejecución detectado es el resultado de una actividad maliciosa.

Integraciones para la respuesta a incidentes

Cuando se produce un incidente, una solución de seguridad de las API debe incluir las integraciones necesarias para garantizar que las tareas de corrección se asignan a los equipos adecuados. Si se detectan errores de configuración, infracciones de políticas de datos o comportamientos sospechosos, se debe informar de ellos a la puerta de enlace de API, el sistema de SIEM y otros motores de seguridad de la información para garantizar el nivel adecuado de difusión.

Como norma general, una solución de seguridad de las API debe integrarse fácilmente con el resto de herramientas de seguridad, supervisión y gestión que utiliza su organización.

Pruebas de seguridad de las API: análisis detallado de las capacidades clave

Un error que cometen muchos equipos de desarrollo es esperar demasiado para comenzar las pruebas de API, de modo que las pruebas acaban convirtiéndose en un cuello de botella. Los equipos deben adoptar una estrategia "shift-left" para garantizar que las pruebas comienzan lo suficientemente pronto en el proceso de desarrollo para garantizar que sean exhaustivas. Las ventajas de unas pruebas eficaces de seguridad de las API son significativas:

- **Prevención de ataques**
  - Al detectar las vulnerabilidades antes de poner las API en funcionamiento, reduce el riesgo de que un ataque logre su objetivo.
- **Mejora del cumplimiento**
  - Las pruebas exhaustivas le ayudarán a garantizar el cumplimiento y a evitar multas y daños a la reputación.
- **Incremento de la confianza**
  - Las pruebas rigurosas y eficaces pueden aumentar la confianza de su organización en las API y ayudar a garantizar que los desarrolladores cumplan sus plazos de lanzamiento.

Algunos proveedores del mercado pueden ofrecer recomendaciones a las empresas sobre cómo solucionar problemas en sus entornos y habilitar configuraciones exhaustivas de pruebas de API. Las recomendaciones pueden incluir pasos para configurar mecanismos de autenticación adecuados o corregir dependencias de API. Y, si puede abordar problemas de lógica empresarial en su entorno, puede aumentar el número de API optimizadas para las pruebas, lo que permite aumentar la cobertura de las pruebas.

Sin embargo, el propio concepto de poner a prueba la seguridad de las API sigue siendo algo confuso. Es posible que los equipos de desarrollo no comprendan del todo lo que implica. El modelo "shift-left" para las pruebas de API es un proceso de tres pasos:

1. **Comprender la API:** entender para qué se va a usar una API ayuda a orientar las pruebas, especialmente en el caso de problemas de lógica empresarial complicados.
2. **Garantizar que es posible interactuar correctamente con la API:** asegúrese de que puede utilizar la API como estaba previsto. Esto es esencial para validar que la idea que tiene sobre la API coincide con cómo funciona realmente.
3. **Enviar tráfico de ataque a la API:** esto podría incluir manipular manualmente las solicitudes a la API, introducir cadenas de fuzzing en las solicitudes o usar una herramienta automatizada para realizar pruebas de seguridad de la API. Como ocurre con casi todo en los entornos de TI modernos, la automatización suele ser la mejor manera de realizar estas tareas a escala y sin comprometer la velocidad.

Funciones clave de pruebas de seguridad de las API

Las pruebas de seguridad de las API deben incluir pruebas estáticas, dinámicas y de penetración. Una solución de seguridad de las API debe incluir herramientas para facilitar pruebas exhaustivas y automatizar los procesos de pruebas en la mayor medida posible. Busque una solución de seguridad de las API con las siguientes funciones de pruebas de API:

Pruebas de seguridad de las API automatizadas y proactivas

Las pruebas de seguridad automatizadas reducen significativamente el riesgo y los costes al identificar errores de configuración, vulnerabilidades e infracciones del cumplimiento antes de que una API se ponga en funcionamiento.

Control de las API

Es fundamental considerar cuestiones relacionadas con la gobernanza como los roles, las responsabilidades y las políticas. Esto incluye las responsabilidades de los encargados de la ejecución, como los desarrolladores, ingenieros de seguridad e ingenieros de plataforma, y la supervisión de las políticas y la toma de decisiones sobre riesgos. Una solución de seguridad de las API debe permitirle analizar las especificaciones de sus API con respecto a las políticas y normativas de control establecidas.

Integración en los procesos de CI/CD y los repositorios de código

DevSecOps es una variante de DevOps que añade la seguridad al flujo de trabajo de desarrollo de software. La seguridad de las API debe formar parte de las iniciativas de DevSecOps. Una solución de seguridad de las API debe proporcionar un conjunto de pruebas de seguridad centradas en las API que se ejecuten bajo demanda o como parte de un proceso de CI/CD. La integración en CI/CD es esencial porque permite realizar de forma rápida y periódica las pruebas de seguridad de las API necesarias para seguir el ritmo del desarrollo de aplicaciones.

Conclusión: Identifique y aborde las brechas en la seguridad de sus API

Las API son un componente esencial de la capacidad de las organizaciones para prestar servicio a los clientes, generar ingresos y trabajar de forma eficiente en una economía cada vez más digital y centrada en la nube. Sin embargo, su crecimiento continuo, su proximidad a los datos confidenciales y la falta de controles de seguridad hacen que las API sean un objetivo atractivo para los atacantes de hoy en día.

Las herramientas que muchas organizaciones utilizan actualmente para gestionar las API y obtener una protección básica reducen en cierta medida los riesgos. Pero no lo suficiente para enfrentarse a las amenazas actuales a las API. No se puede confiar en ellas como única fuente de protección.

En su lugar, las organizaciones deben buscar una solución completa de seguridad de las API que pueda proporcionar los cuatro componentes descritos en esta guía del comprador: detección, gestión de la estrategia, detección y corrección de amenazas y pruebas de seguridad. No tiene que prescindir de las herramientas que ya tiene y que han demostrado ser eficaces en determinadas áreas, solo tiene que buscar una solución que se pueda integrar a la perfección con esas herramientas.

Cuando dé sus primeros pasos en lo que respecta a la seguridad de las API, no hace falta que asigne una cantidad considerable de recursos. Puede empezar por un programa piloto cuantificable y a pequeña escala que aborde las brechas específicas de su pila de seguridad. O puede iniciar su experiencia en seguridad de las API con una actualización completa. Cada organización es diferente.

Con los ataques dirigidos a API en auge, el paso más importante es la decisión de tomar medidas. Esperamos que esta guía del comprador le haya resultado útil.

Obtenga más información sobre
los métodos de ataque a las API,
las vulnerabilidades comunes de las API
y las formas de proteger su organización.

Descubra cómo podemos ayudarle
con esta **demostración de Akamai
API Security personalizada**.

La seguridad de Akamai protege las aplicaciones que impulsan su negocio en cada punto de interacción sin comprometer el rendimiento ni la experiencia del cliente. Gracias a la escala de nuestra plataforma global y su visibilidad de las amenazas, colaboramos con usted para prevenirlas, detectarlas y mitigarlas, de forma que pueda generar confianza en la marca y cumplir su visión. Para obtener más información acerca de las soluciones de cloud computing, seguridad y distribución de contenido de Akamai, visite **akamai.com** y **akamai.com/blog**, o siga a Akamai Technologies en **X**, antes conocido como Twitter, y **LinkedIn**. Publicado en septiembre de 2024.

Akamai