CEQUENCE SECURITY

FICHA DE DATOS

Cequence Bot Defense

Prevención de ataques API basada en ML

Introducción

Los atacantes adoran las API por las mismas razones por las que los desarrolladores las adoran. Son fáciles de usar, flexibles y rápidos. Esos hechos, junto con un rico depósito de credenciales robadas, kits de herramientas de ataque e infraestructura comprometida, han facilitado que los malhechores ejecuten apropiaciones de cuentas y abusos de lógica comercial contra sus API y aplicaciones web que pueden resultar en fraude o robo. Estos ataques automatizados se esconden a simple vista, enmascarados como transacciones legítimas, lo que dificulta mucho la decisión de bloquear o no para los equipos de seguridad. Las organizaciones necesitan una solución abierta y extensible que permita una respuesta rápida a los ataques basados en API cada vez más agresivos, como compras y raspado automatizados, así como ATO y creación de cuentas falsas.

Visión general

Bot Defense es la única oferta de mitigación de bots que no requiere ninguna integración de JavaScript o SDK móvil para recopilar la telemetría de ataque necesaria para evitar ataques de bots automatizados maliciosos que pueden provocar fraude o pérdida de datos. Bot Defense aprovecha CQAI, un motor de análisis patentado que descubre todas las API y aplicaciones web para crear un mapa visual del sitio. Las solicitudes de aplicaciones luego son analizadas por los modelos basados en ML patentados de CQAI para detectar ataques automatizados maliciosos que luego pueden mitigarse de forma nativa, en tiempo real.

Funciones de defensa contra bots

Prevención de amenazas API basada en el comportamiento

Bot Defense está impulsado por CQAI, un motor de análisis basado en ML sin agentes que se basa en la mayor base de datos de amenazas de comportamientos de amenazas de API y registros de infraestructura maliciosa del planeta. Cada una de sus transacciones de API y aplicaciones web son analizadas por CQAI utilizando cientos de reglas predefinidas que dan como resultado una huella digital de comportamiento única que rastrea continuamente ataques sofisticados, incluso cuando se modifican para evitar la detección. El resultado es una protección de API y aplicaciones web de alta eficacia contra toda la gama de ataques automatizados según lo definido por OWASP.

El enfoque basado en ML sin agente ofrece dos beneficios clave. En primer lugar, integra de forma efectiva la seguridad en el flujo de trabajo de su aplicación, eliminando la instrumentación de JavaScript de la aplicación y las penalizaciones de integración de SDK móvil, como demoras en la implementación y tiempos lentos de carga de páginas. El segundo beneficio proporcionado es una protección consistente contra ataques automatizados contra las API y sus aplicaciones web, lo que elimina de manera efectiva las posibles brechas de seguridad causadas por las redirecciones de tráfico engorrosas y la inserción de cookies.

Defensa contra bots de un vistazo

Protección de API y aplicaciones web de alta eficacia contra toda la lista de amenazas automatizadas de OWASP. Los beneficios clave incluyen:

- **Reduce los impactos comerciales** causados por apropiaciones de cuentas, creación de cuentas falsas, compras automatizadas, raspado de contenido/precio y fraude con tarjetas de regalo.
- **Acelera el tiempo de respuesta a incidentes**con visibilidad completa de los ataques automatizados contra las API y las aplicaciones web.
- **Reduce los esfuerzos administrativos de la política**y mejora la postura de seguridad con una protección consistente tanto para las aplicaciones web como para las API.
- **Modelo de implementación de SaaS discreto**permite una protección de alta eficacia en minutos, no semanas o años.

k El producto Cequence [AI] Bot Defense eclipsa al resto con su SDK de hazaña más destacado. Se implementa rápidamente en una infraestructura de AWS con múltiples opciones para tomar decisiones en función de las políticas que escriba.

Vicepresidente de Seguridad de la Información,
Empresa minorista/de subastas, revisión de 5 estrellas de Gartner Peer Insights

ure: No es necesario integrar un H alimentación de su tráfico en tiempo real

Reglas, políticas y opciones de respuesta personalizables

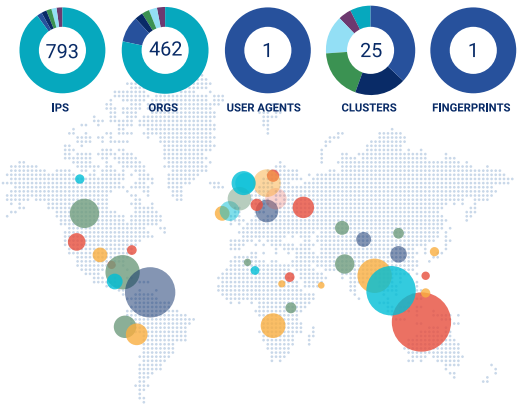
Usando reglas personalizables y listas para usar, los hallazgos de CQAI se pueden traducir en políticas que aplican un modelo de seguridad positivo, lo que permite lo que desea y niega todo lo demás. A diferencia de las ofertas alternativas que requieren servicios profesionales para acceder a los datos o realizar otros cambios, la creación y administración de políticas puede ser realizada por su equipo o en conjunto con el Servicio de Monitoreo de Amenazas de Cequence con el apoyo brindado por nuestro Equipo de Investigación de Amenazas de CQ Prime. Los ataques descubiertos se pueden mitigar utilizando una variedad de opciones de respuesta que incluyen bloqueo, limitación de velocidad, cercado geográfico y engaño, una técnica que le permite engañar y engañar al atacante haciéndole creer que sus ataques han tenido éxito.

Una base de datos de millones de registros de amenazas

La protección de su API y aplicación web está respaldada por la base de datos de amenazas de API más grande del planeta. Los registros incluyen comportamientos de ataque, infraestructura maliciosa, credenciales robadas y kits de herramientas, todos los cuales son seleccionados por el equipo de investigación de amenazas de CQ Prime en reglas listas para usar que brindan una protección de alta eficacia. Las reglas se pueden personalizar para cumplir con los requisitos únicos del cliente y los patrones de ataque en constante cambio.

Asociación de monitoreo de amenazas

Bot Defense es una solución abierta y ampliable con una interfaz gráfica de usuario enriquecida que permite a su equipo analizar rápidamente los ataques, tomar decisiones sobre políticas y generar informes. La administración granular basada en roles le permite controlar a qué funciones pueden acceder los miembros de su equipo. En caso de que su equipo necesite ayuda, nuestro equipo de investigación de amenazas de CQ Prime está aquí para ayudarlo, ya sea para brindar orientación y aportes periódicos, o como una extensión de servicio con licencia de su equipo donde trabajan codo con codo para prevenir amenazas. Es tu elección.



Se integra fácilmente con la infraestructura existente

Las API basadas en REST le permiten importar datos de terceros para mejorar el análisis de CQAI, o puede exportar los hallazgos a su infraestructura de TI existente para el análisis post-mortem, la correlación o la aplicación por parte de su firewall u otro dispositivo de seguridad.

Se implementa en minutos

Bot Defense SaaS se puede habilitar para proteger sus aplicaciones web y API en tan solo 15 minutos y puede comenzar a reducir inmediatamente la carga operativa asociada con la prevención de ataques que pueden resultar en fraude o pérdida de datos. Como alternativa, la arquitectura modular basada en contenedores permite que Bot Defense se implemente en su centro de datos, su entorno de nube o como un híbrido.

Bot Defense y la solución de protección API unificada

Como componente integral de la solución Unified API Protection, Bot Defense complementa API Spyder y API Sentinel con detección y prevención basadas en ML de ataques automatizados contra sus API y aplicaciones web. 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 del ciclo de vida de seguridad de su 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.

CEQUENCE SECURITY
100 Murphy Avenue, Suite 300, Sunnyvale, CA 94086 1>650-437-6338 info@cequence.ai www.cequence.ai