transparent edge

www.transparentedge.eu
comercial@transparentedge.eu
+ 34 91 091 64 19

MEJORAMOS EL MUNDO DEFINIDO POR INTERNET

La CDN europea que te pone las cosas fáciles

DETECCIÓN DE ANOMALÍAS

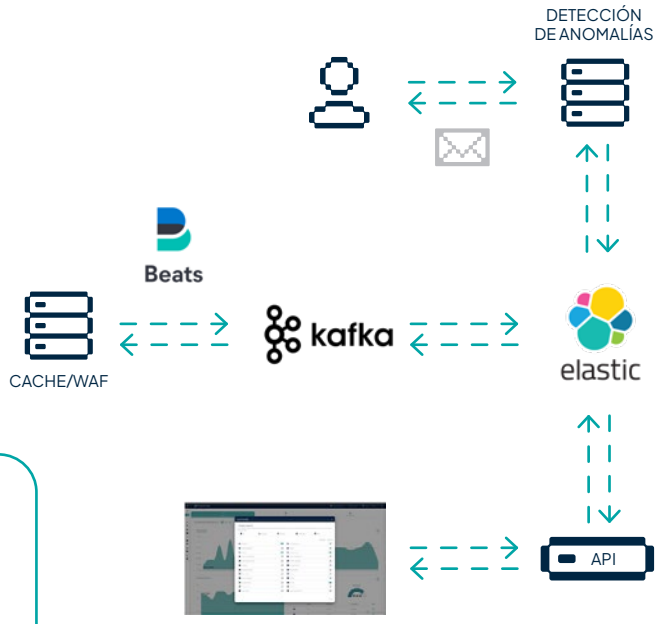
Visibilidad completa de tu entorno

La detección de anomalías es esencial en la estrategia de ciberseguridad actual debido a la sofisticación, disrupción y frecuencia de una nueva generación de amenazas. Estos sistemas analizan patrones e identifican alteraciones en el tráfico que pueden ser signo de un incidente en curso. Reconocer estas anomalías a tiempo permite actuar de manera preventiva en muchas ocasiones y adelantarse a un incidente más grave.

El sistema de detección de anomalías de Transparent Edge es un servicio que busca patrones en el tráfico de tus sitios web, notifica si se producen anomalías y ofrece la posibilidad de accionar nuestros sistemas para, llegado el momento, reaccionar a un incidente, por ejemplo, cuando estás sufriendo un ataque de Denegación de Servicio Distribuido (DDoS).

Cómo funciona el sistema de anomalías de Transparent Edge

Basado en nuestra herramienta de analítica avanzada, el sistema permite ver minuciosamente qué está pasando en tiempo real por tu sitio web. Contamos con una arquitectura muy potente para ofrecer un alto nivel de detalle.



VENTAJAS DEL SISTEMA DE DETECCIÓN DE ANOMALÍAS

1

Las detecciones pueden configurarse fácilmente desde nuestro panel de control. El servicio permite activar o desactivar las detecciones para cada uno de tus sitios, además de poder configurar los parámetros de detección de manera individual al personalizar su umbral y sensibilidad en función de la naturaleza de cada web.

2

Este servicio está integrado con nuestro sistema de gestión de ACL, de manera que si una IP de confianza está haciendo saltar alguna anomalía, esta puede ser incluida en una lista para que no se tenga en consideración.

Anomalías detectadas por el sistema de Transparent Edge

INCREMENTO EN EL TRÁFICO

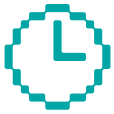
Basándonos en percentiles 95, analizamos el tráfico en busca de un incremento de peticiones o de ancho de banda. Además, el sistema busca patrones similares en el pasado para determinar si se trata de una anomalía o de un evento recurrente. Esta detección, junto con la de *requests* por IP es muy útil para identificar DDoS.

HIT RATIO

El sistema detecta cuando el *hit ratio* de tu web desciende de manera brusca. Esto puede ser debido a varios factores, por ejemplo: un cambio en las políticas de cacheo o que alguien esté intentando atacar tu origen saltándose la caché con parámetros aleatorios.

REQUEST POR IP

Se basa en el cálculo de la media de peticiones por segundo que tiene cada usuario de tu web. Te avisa cuando las peticiones por segundo de una IP superan tres veces la desviación estándar, siempre que esté por encima del umbral de sensibilidad permitido.



TIEMPO DE RESPUESTA

Te alerta cuando la plataforma de origen está tardando en responder y los tiempos de respuesta se disparan por encima de lo normal. Esta detección también se basa en una distribución normal para identificar esos tiempos de respuesta por encima de lo permitido.

CÓDIGO DE ESTADO

Notifica cualquier incremento sustancial de errores 503 en tu sitio web. Monitorizar este tipo de errores tiene sentido porque en Transparent Edge todos los errores 50× son enmascarados con un status code 503.

ESCÁNER DE VULNERABILIDADES

Esta detección alerta cuando algún usuario malintencionado está tratando de escanear tu sitio web en busca de vulnerabilidades en tú código, de manera que cuando esto ocurra puedas tomar decisiones de forma automática o manual. Te alerta incluso cuando el WAF se encuentra en modo detección.

OTROS PRODUCTOS RECOMENDADOS

Todas las áreas del ecosistema de TI están expuestas a un ciberataque en mayor o menor medida. Lidiar a diario con cientos de ellos, nos permite desarrollar soluciones de seguridad que incluyen distintas tecnologías de detección y mitigación eficiente de amenazas.

WAF

- Inyección de SQL (SQL Injection), XSS y CSRF
- Amenazas avanzadas más allá del top 10 de OWASP
- Apropiación de cuentas (ATO)
- Soporte de varios niveles de seguridad
- Modo estricto y modo solo detección
- Cifrado TLS
- *Bot detection (captcha, cookie, Javascript)*
- *Rate limit*
- Firmas personalizadas

BOT MITIGATION

- IPs con baja reputación
- *Datacenters* de baja reputación
- ASN de baja reputación
- Listas de abuso
- VPNs
- Redes TOR
- Redes *Proxy* anónimos
- Lista de *bogons*

ANTI-DDOS

- En capas 3 y 4
  - → Inundación de negociación SSL, UDP, GRE-IP UDP, SYN, TCP RST,
  - → TCP CONNECT() y TCP ACK
  - → Amplificación de DNS, NTP, CharGEN, Memcache, SSD, SNMP
  - → Tsunami SYN
  - → Ataques de fragmentación y CLDAP
  - → ARMS (ARD)
  - → *Jenkins*
  - → Cuentagotas DNS
  - → CoAP
  - → WS-DD
  - → NetBIOS
- En capa 7
  - → Inundación de peticiones HTTP/S, de inicio de sesión, de creación
  - → de sesión y de contenido
  - → Amplificación DNS
  - → Ataques de fuerza bruta
  - → *Slowlories*