La guía de los defensores de 2025

Fortalezca sus defensas para el futuro

Anticípese a los vectores de ataque emergentes y a las nuevas formas de cargar contra objetivos antiguos. Empiece por leer lo más destacado de nuestra antología "La guía de los defensores".

Organice sus defensas para garantizar una seguridad exhaustiva

Existen tres pilares fundamentales:

Gestión de riesgos para priorizar las respuestas según la probabilidad de una amenaza específica y la capacidad de esas respuestas para reducir la vulnerabilidad de la empresa.

Arquitectura de red para implementar un sistema de seguridad de varios niveles a través de firewalls, segmentación y controles de acceso para contener posibles filtraciones.

Seguridad del host para proteger los dispositivos individuales del malware y el acceso no autorizado mediante actualizaciones del sistema, software antivirus, firewalls y controles de acceso.

¿Dónde podría ocultarse el malware?

Principales protocolos asociados a incidentes de puertos abiertos en 2024

58,0 %
Protocolo de bloques de mensajes del servidor (SMB)

14,5 %
Protocolo de escritorio remoto (RDP)

12,9 %
Protocolo de comunicaciones seguras (SSH)

¿Qué pueden hacer los atacantes al acceder a una VPN?

- Utilizar un servidor de autenticación remoto para autenticar a los usuarios
- Utilizar la autenticación legítima a su antojo
- Utilizar servidores de autenticación fraudulentos
- Extraer y descifrar los secretos del archivo de configuración

Evite las vulnerabilidades XSS

- Añada codificación de salida en todos los parámetros controlados por el usuario.
- Proteja su empresa con el método de revisión del código y los firewalls de aplicaciones web.
- Detenga las tácticas reales de los ciberdelincuentes, como el robo de cookies, la desfiguración en los sitios web y la falsificación de sesiones o solicitudes entre sitios.

¿Por qué los contenedores son el objetivo principal de los atacantes?

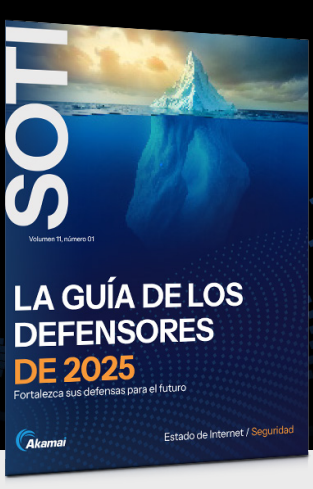
Los investigadores de Akamai identificaron varias vulnerabilidades y tácticas en Kubernetes que, si se explotan, pueden dar lugar a:

- Exfiltración de datos
- Derivación de privilegios
- Ejecución remota de código

Combine medidas preventivas con una preparación para responder eficazmente

Estos son los cuatro principios fundamentales:

- Implemente la ciberhigiene en todas partes.
- Implemente un sistema de protección por capas en todo su entorno utilizando diferentes plataformas de seguridad.
- Céntrese en los servicios esenciales de su empresa .
- Asegúrese de contar con un equipo o partner de confianza para responder a los incidentes.



Descargar "La guía de los defensores de 2025"

| Publicado en febrero de 2025