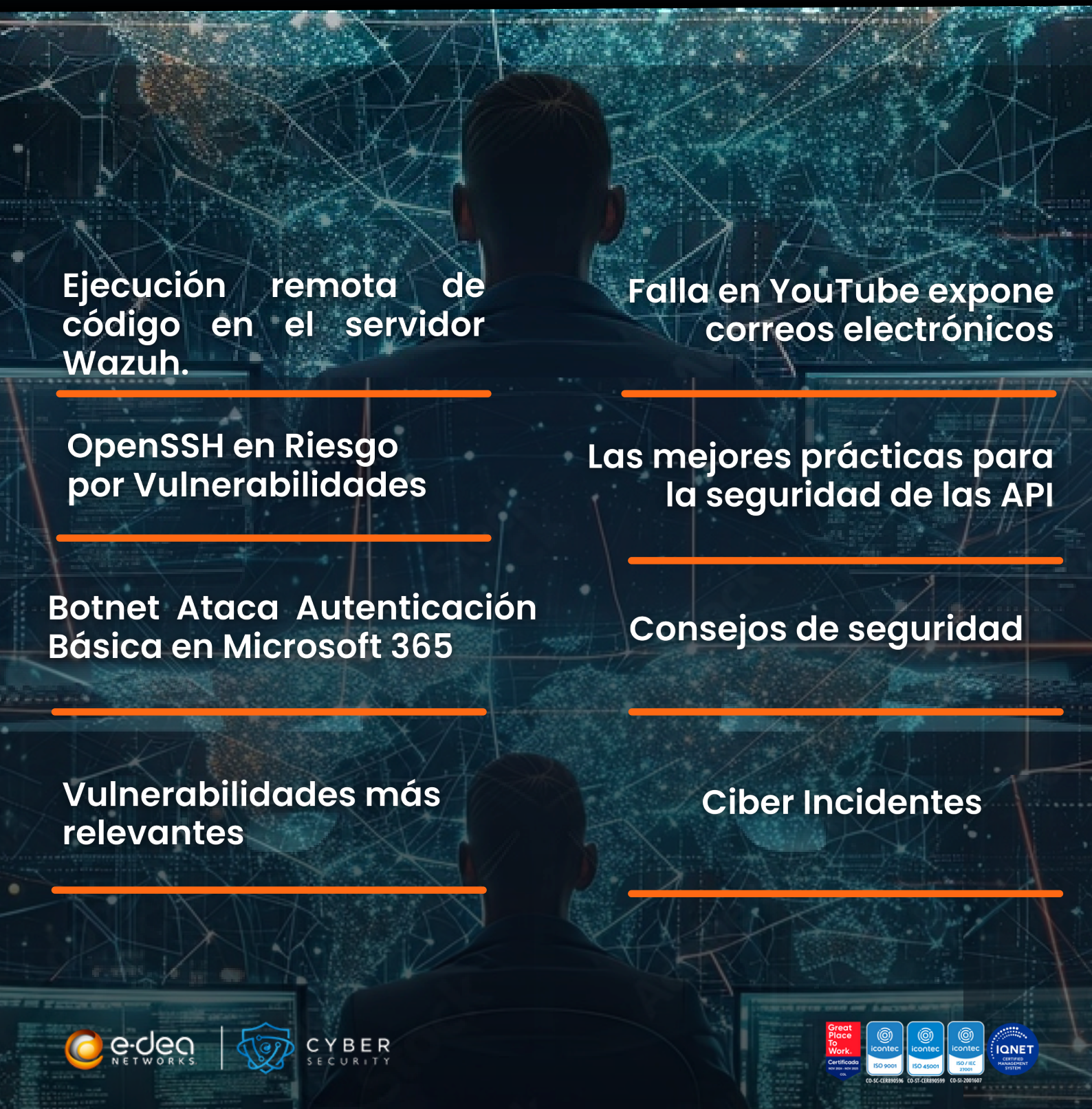
Edición 6 Febrero 2025

CIBER E-DEA

Boletín de Seguridad



Ejecución remota de código en el servidor Wazuh.

Falla en YouTube expone correos electrónicos

OpenSSH en Riesgo por Vulnerabilidades

Las mejores prácticas para la seguridad de las API

Botnet Ataca Autenticación Básica en Microsoft 365

Consejos de seguridad

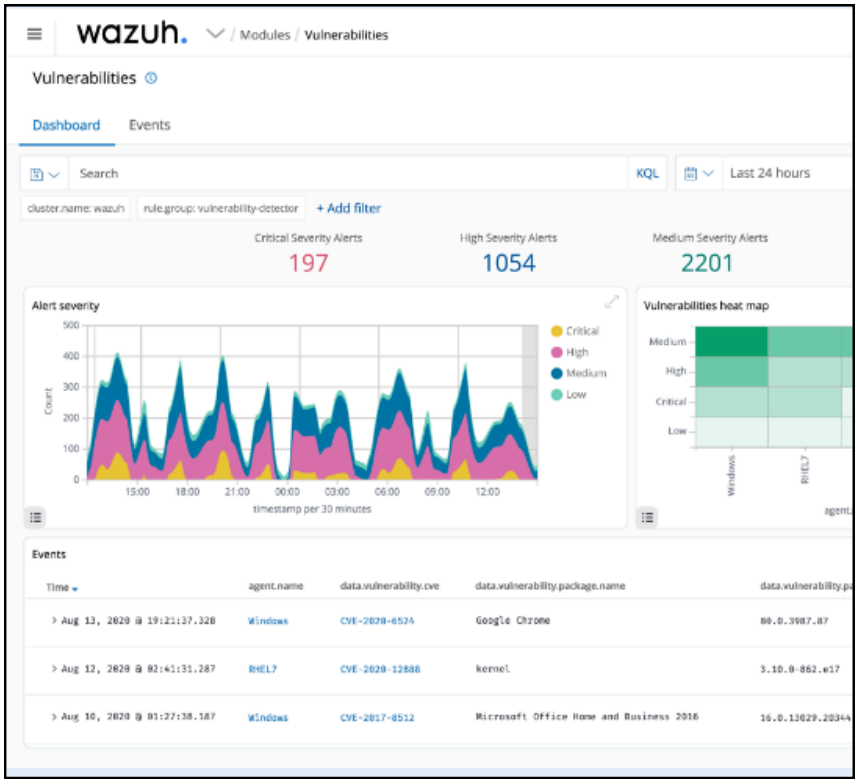
Vulnerabilidades más relevantes

Ciber Incidentes

e-dea NETWORKS | CYBER SECURITY

Ejecución remota de código en el servidor Wazuh.

El equipo de Wazuh ha emitido una alerta de seguridad sobre una grave vulnerabilidad en su plataforma de seguridad. Identificada como CVE-2025-24016 , esta falla ha recibido un puntaje de 9.9 en el sistema CVSS , lo que la clasifica como crítica. La vulnerabilidad permite que un atacante ejecute código de manera remota en servidores afectados, comprometiendo por completo su integridad y seguridad.



Detalles técnicos

Wazuh es una solución de código abierto utilizada para detección de amenazas, monitoreo de integridad de archivos, análisis de registros y respuesta ante incidentes. Sin embargo, CVE-2025-24016 explota una falla de deserialización insegura en la API del servidor Wazuh , permitiendo que un atacante ejecute comandos arbitrarios mediante el envío de una solicitud especialmente diseñada.

Se ha publicado un exploit de prueba de concepto (PoC) que muestra la facilidad con la que se puede explotar esta vulnerabilidad para apagar un servidor maestro:

```
curl -X POST -k -u "wazuh-wui:MyS3cr37P450r.*-" -H "Content-Type: application/json" --data '{"__unhandled_exc__":{"__class__": "exit", "__args__": []}}' https://<worker-server>:55000/security/user/authenticate/run_as
```

Versiones afectadas

Se ha confirmado que los atacantes han explotado activamente las versiones 4.4.0, 4.7.2 a la 4.9.1 , lo que aumenta la urgencia de actualizar a la versión corregida.

Más información

Falla en YouTube expone correos electrónicos

Una vulnerabilidad crítica en la infraestructura de YouTube permitió a los atacantes exponer las direcciones de correo electrónico vinculadas a canales anónimos mediante la combinación de fallas en el sistema de administración de cuentas de Google y una API Pixel Recorder obsoleta.

Las fallas fueron descubiertas por los investigadores de seguridad Brutecat y Nathan quienes encontraron que las API de YouTube y Pixel Recorder podrían usarse para obtener los ID Gaia de Google de los usuarios y convertirlos en sus direcciones de correo electrónico.

El ataque se inició aprovechando el sistema de moderación del chat en vivo de YouTube. Los investigadores encontraron que al abrir el menú contextual (mediante el botón de tres puntos) en el mensaje de chat en vivo de un usuario, se activaba una solicitud de API.

Esta solicitud devolvía un parámetro codificado en base64 que contenía el ID de Gaia ofuscado del objetivo, un identificador único de cuenta de Google destinado a uso interno

```
( /youtubei/v1/live_chat/get_item_context
_menu).
```

Respuesta de Google:

Google confirmó que había mitigado el problema al aplicar parches tanto a la API de YouTube como al mecanismo de uso compartido de Pixel Recorder.

Además, el bloqueo de usuarios en YouTube ahora solo afecta las interacciones dentro de esa plataforma y no expone los ID de Gaia en otros servicios.

También aseguró a los usuarios que no había evidencia de explotación activa de estas fallas antes de que fueran solucionadas el 9 de febrero de 2025.

Recomendaciones:

- Mantener la cuenta de YouTube separada de otras cuentas personales o corporativas.
- Cambiar la contraseña regularmente.
- Habilitar el MFA o 2FA a las cuentas.

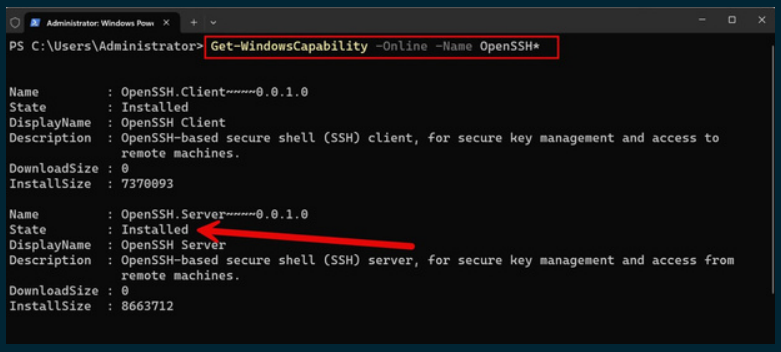
Mas información

OpenSSH en riesgo por nuevas vulnerabilidades

Se han identificado dos vulnerabilidades críticas en OpenSSH, exponiendo a millones de servidores a ataques de intermediarios (MITM) y denegación de servicio (DoS). OpenSSH ha lanzado la versión 9.9p2 para corregir estos fallos.

Detalles de las Vulnerabilidades

CVE-2025-26465 (MITM): Permite a atacantes en ruta suplantar servidores, comprometiendo la integridad de sesiones SSH y exponiendo credenciales.
CVE-2025-26466 (DoS): Provoca un consumo excesivo de memoria y CPU mediante paquetes SSH2_MSG_PING, afectando clientes y servidores.



Impacto y Alcance

Las vulnerabilidades afectan diversas versiones de OpenSSH, una implementación de código abierto del protocolo Secure Shell 2.0 utilizada para acceso remoto y gestión de servidores.

OpenSSH está presente en sistemas como Microsoft Windows 10 y 11, macOS y la mayoría de las distribuciones de Linux.
El motor de búsqueda Shodan ha detectado aproximadamente 33 millones de servidores expuestos que ejecutan OpenSSH, aunque no todos son necesariamente vulnerables. Para mitigar los riesgos, el proyecto OpenSSH ha lanzado la versión 9.9p2, corrigiendo los fallos.

Recomendaciones

Se insta a actualizar a OpenSSH 9.9p2 de inmediato y verificar configuraciones para mitigar riesgos. La pronta aplicación de parches es clave para la seguridad y disponibilidad de los sistemas.

Más información

Las mejores prácticas para la seguridad de las API

Los entornos de aplicaciones web se están volviendo más complejos y difíciles de proteger. Dado que las aplicaciones residen cada vez más en la nube, se encuentran en contenedores, se conectan a través de API y se entregan mediante CDN, mantener medidas de seguridad sólidas es más crítico que nunca.

Las API definen reglas y protocolos que permiten que las aplicaciones se comuniquen y compartan datos con otros sistemas. Esta comunicación permite a los desarrolladores aprovechar la funcionalidad de las aplicaciones existentes en lugar de recrear esas funciones y servicios desde cero. Como resultado, las API aceleran el desarrollo de software y permiten la innovación, la colaboración y la automatización.

Identificación de riesgos y amenazas comunes para proteger eficazmente sus API, es fundamental comprender los riesgos y amenazas comunes que existen, incluidos:

- Ataques de inyección
- Explosiones de vulnerabilidades
- Problemas de autenticación
- Controles de acceso rotos
- Denegación de servicio distribuida (DDoS)
- Ataques de fuerza bruta
- Abuso de API
- Ataques de tipo máquina en el medio (MITM)
- Scripts entre sitios (XSS)

Defensa Proactiva

Metodologías de Desarrollo Seguro
DevSecOps
SSDLC
OWASP SAMM
SAST

Descubrimiento de API

Identifique las API inactivas, heredas o zombis, mantenga un inventario actualizado

Manejo de la postura

Evalué las API y la infraestructura en busca de configuraciones incorrectas y vulnerabilidades

Autenticación y Autorización

MFA - OAuth 2.0
API Key
JWT
RBAC

Seguridad de Datos

TLS para conexiones
AES – RSA para BD

Manejo de incidentes

Tenga un plan de respuesta a incidentes
Mantenga su API y sistemas back-end actualizados

Auditorias

Programe auditorias periódicas por parte de externos

Protección en Tiempo de Ejecución
OWASP TOP 10 API
Monitoree tráfico de las API
Detección de amenazas basada de firmas

Pruebas de Seguridad y Cumplimiento

OWASP TOP 10 API

Gestión de configuración

Ciclo de vida SSDLC
Versionamiento

Gestión de superficie de Ataque

Habilite CSP
Utilice HSTS
X-content-type-options

Aplicaciones de seguridad para API

Gateway API
WAF

Más de 130,000 dispositivos en una Botnet atacan cuentas de M365

Se trata de un **tipo de ataque de fuerza bruta en el que un actor malicioso intenta utilizar la misma contraseña en varias cuentas** antes de pasar a probar con otra.
Los actores de amenazas apuntaron contra **cuentas protegidas con autenticación básica** que eludían la autenticación multifactor.

La botnet, controlada por un grupo afiliado a China, utiliza credenciales robadas por malware de robo de información para lanzar ataques a gran escala. Los atacantes se enfocan en sistemas que aún utilizan la autenticación básica, lo que les permite eludir las protecciones de MFA. Una vez que obtienen acceso a las cuentas, pueden robar datos sensibles, interrumpir operaciones comerciales y moverse lateralmente dentro de la organización objetivo.

Recomendaciones

Para mitigar estos ataques, se recomienda deshabilitar la autenticación básica en Microsoft 365, monitorear patrones de inicio de sesión inusuales y habilitar políticas de acceso condicional (CAP) para restringir los intentos de inicio de sesión. Además, es crucial mantener una buena higiene cibernética y capacitar a los empleados sobre las mejores prácticas de seguridad para reducir el riesgo de compromisos.

Más información

Cómo evitar un ataque cibernético y cuáles son los más comunes

Un ataque cibernético es cualquier intento malintencionado de acceder, dañar o robar información digital a través de sistemas informáticos, redes o dispositivos conectados a Internet

Tipos más comunes de ataques cibernéticos

Existen diversos tipos de ataques cibernéticos, cada uno con sus propias características y métodos de ejecución. A continuación, te presentamos los más frecuentes:

El phishing es un ataque en el que se envían mensajes falsos para engañar a la víctima y obtener información sensible

El ransomware bloquea el acceso a archivos hasta que se paga un rescate.

El malware es software malicioso diseñado para dañar sistemas,.

los ataques Man-in-the-Middle, el hacker intercepta la comunicación entre dos partes para robar o manipular información.

El spyware se instala en un dispositivo sin el conocimiento del usuario para monitorear su actividad y robar datos confidenciales.

Cómo evitar un ataque cibernético

Protegerte de los ataques cibernéticos no tiene por qué ser complicado. Aquí tienes algunas medidas básicas que puedes tomar:

- Usa contraseñas fuertes: Combina letras, números y símbolos, y evita usar la misma contraseña para múltiples cuentas.
- Mantén tu software actualizado: Las actualizaciones suelen incluir parches de seguridad que protegen contra vulnerabilidades.
- Instala un antivirus confiable: Un buen antivirus puede detectar y bloquear amenazas antes de que causen daños.
- Evita enlaces sospechosos: No hagas clic en enlaces o descargues archivos de fuentes desconocidas.
- Usa redes seguras: Evita conectarte a redes Wi-Fi públicas sin protección, especialmente para realizar transacciones bancarias.

Vulnerabilidades destacadas

CVE-2025-21391

Microsoft - Windows

Versiones afectadas

Todas las versiones.

Un atacante local y autenticado podría aprovechar esta vulnerabilidad para eliminar archivos de un sistema. Según Microsoft, esta vulnerabilidad no revela información confidencial a un atacante, sino que solo le brinda la capacidad de eliminar datos, que pueden incluir datos que podrían provocar la interrupción del servicio.

CVE-2025-24085

Apple

Versiones afectadas

iOS 17.2

Se han descubierto múltiples vulnerabilidades en productos de Apple, la más grave de las cuales podría permitir la ejecución de código. La explotación exitosa podría otorgar a un atacante la capacidad de instalar programas, modificar o eliminar datos, y crear nuevas cuentas con privilegios elevados.

CVE-2025-0111

Paloalto

Versiones afectadas

PAN-OS

Esta vulnerabilidad permite la ejecución remota de código (RCE) sin autenticación, lo que significa que un atacante podría tomar el control del firewall sin necesidad de credenciales válidas. Una vez comprometido, el atacante podría modificar configuraciones, crear puertas traseras o interrumpir servicios esenciales de la red.

Ciber incidentes en Colombia y en el mundo

Aumento de Ciberataques en 2025: Un Desafío para la Seguridad Digital

En 2025, los ciberataques han alcanzado niveles sin precedentes, impulsados por el uso de tecnologías avanzadas como la inteligencia artificial (IA). Según el Informe Global de Respuesta a Incidentes 2025 de Unit 42, el 86% de los incidentes cibernéticos más significativos resultaron en interrupciones operativas, daños financieros o afectaciones a la reputación de las empresas

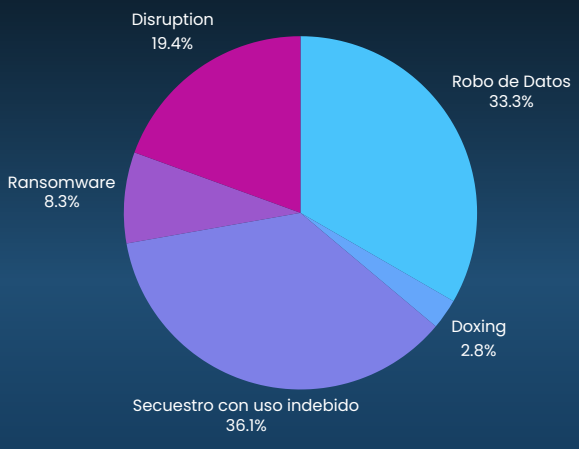
Más información

El mundo

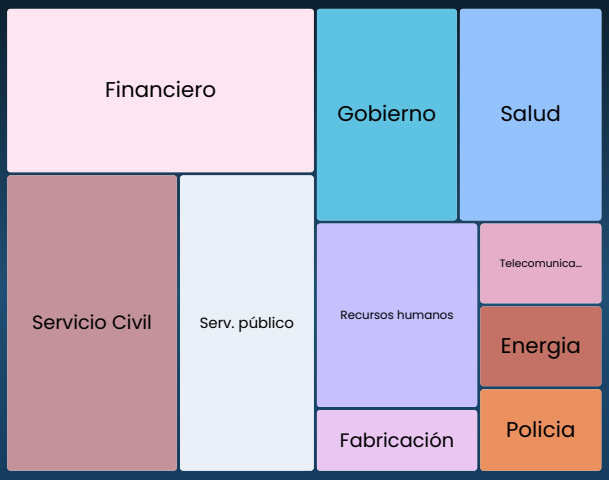
19

Ciber incidentes

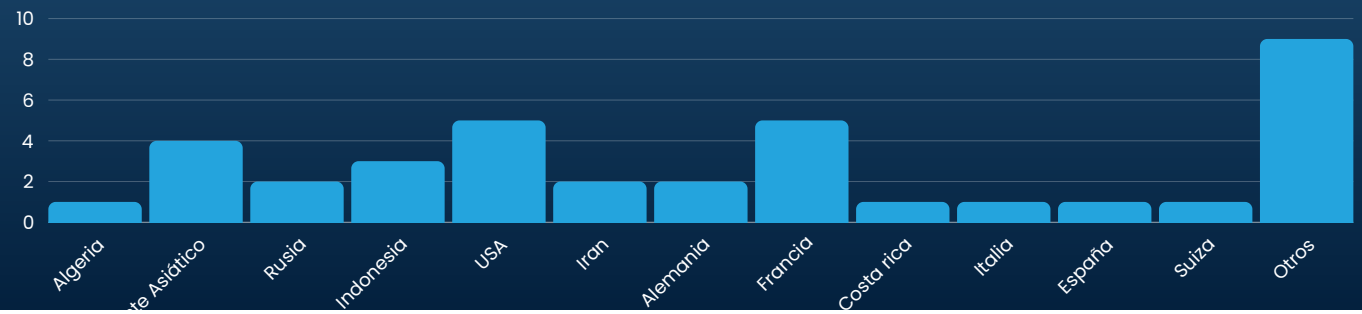
TIPO DE INCIDENTE



SECTORES AFECTADOS



PAISES ATACADOS



Más información

e-dea NETWORKS | SOLARWINDS Elite Partner

Webinar

OBSERVABILITY STRATEGY

El Rol de la Observabilidad en el Futuro Empresarial

Jueves 13 de Marzo

10:00 a.m. CO | 9:00 a.m. MX

¡Regístrate ahora!

CYBER SECURITY

e-dea NETWORKS

CIBER E-DEA

Boletín de Seguridad

E-dea Networks

@e_deanetworks

E-dea Networks

Csirt E-dea

e-dea.co