HACKNOID

COINTIC

Análisis y Gestión de Vulnerabilidades 24/7

Todo tu ambiente tecnológico, monitoreado de forma automática

www.cointic.com.mx

¿Qué es Hacknoid?

Hacknoid es la única plataforma que da visibilidad y prioriza tus vulnerabilidades de forma simple e integral.

Apoyamos tu rol de CISO automatizando la búsqueda y gestión continua de vulnerabilidades en tu ambiente tecnológico permitiéndote abordar el riesgo de forma práctica, simple y preventiva.

EL **IMPACTO FINANCIERO** Y DE **IMAGEN** ES INCALCULABLE

COINTIC

Encuentra tus vulnerabilidades antes que los atacantes

24X7 AUTOMATIZADO

La forma más eficiente de proteger a su empresa contra los ciberataques es automatizando completamente el análisis y la gestión de vulnerabilidades todo los días del año

CONFIGURACIÓN ON-PREMISE, CLOUD O AMBIENTES HÍBRIDOS

Los entornos locales, en la nube o híbridos siempre serán propensos a ciertos riesgos contra los que hay que protegerse con una planificación y configuración adecuada

INTERFASE GRÁFICA ÁGIL Y SIMPLE

Intuitiva interfaz de usuario que te permite empezar a trabajar rápidamente y gestionar riesgos en consecuencia

Trabajo Previo

- Determinar alcance del programa
- Definir roles y responsabilidades
- Seleccionar herramientas para el escaneo
- Crear y refinar políticas y SLAs
- Identificar fuentes de contexto de activos

COINTIC

Ciclo Gestión de Vulnerabilidades

HACKNOID REDUCE EL TRABAJO OPERATIVO DE CIBERSEGURIDAD PERMITIENDO FOCALIZAR ESFUERZOS

COINTIC

Características Hacknoid

FUNCIONAL

90%

90% de las empresas no tienen tiempo ni recursos humanos.

SENCILLO

58%

58% de AHORRO horas hombre por la automatización que se pueden derivar para la ejecución de remediación.

CONTINUO

45%

45% del ESFUERZO se pierde hoy en vulnerabilidades con baja explotabilidad debido a un proceso de priorización incorrecto.

Características Hacknoid

AUTOMATIZANDO LAS PRUEBAS DE VULNERABILIDAD

Las organizaciones pueden mejorar significativamente su seguridad implementando una plataforma de automatización que escanee en modo 24/7 , todo el entorno en busca de vulnerabilidades y otros problemas asociados a riesgos.

Funcional

Automatiza el análisis de vulnerabilidad para todo el entorno TI de forma integral, en modo 24/7.

COINTIC

¿Te resulta complejo abordar la gestión de riesgos tecnológicos?

¡Nosotros nos ocupamos!

VISIÓN SENCILLA DEL ESTADO DE LA SEGURIDAD

Ahora tu equipo de ciberseguridad y TI puede tener en una sola vista el estado de seguridad de todo el entorno, evitando falsos positivos y sin informes tediosos.

El cuadro de mando, muestra de forma sencilla (no ofrecer) a tecnicos y gestores el estado de salud de la ciberseguridad, que con agrupaciones y colores permite identificar rápidamente puntos de mayor criticidad para ordenar la remediación.

Sencillo

Visualiza el estado de la seguridad de toda tu infraestructura tecnológica, por medio de un dashboard de control simple, tanto para técnicos como para gerentes.

COINTIC

Lidera tu gestión de Ciberseguridad

¡Solicita una demo!

Características Hacknoid

EVALUACIÓN CONTINUA DE VULNERABILIDADES

Las vulnerabilidades se reducen al estar permanentemente alerta y tratarlas en una gestión continua, asegurando que el tiempo de convivencia con ellas sea el mínimo posible. Esto provee la base fundamental para la continuidad del negocio, para actuar de forma proactiva y evitar afectar los procesos críticos.

Continuo

Al estar alerta permanentemente, se reduce el tiempo de convivencia con las vulnerabilidades evitando caídas del sistema o presentando momentos críticos.

COINTIC

Minimiza tiempos de exposición

Automatiza la ciberseguridad

Dashboard

Permite una visibilidad integral de lo que ocurre en temas de seguridad, de forma inmediata.

Widget

- Configurable por usuario y rol
- Agrupación flexible de los activos según criticidad, ubicación, o criterio escogido
- Monitoreo con frecuencias granulares y flexibles también según criterios de negocio

Indicadores

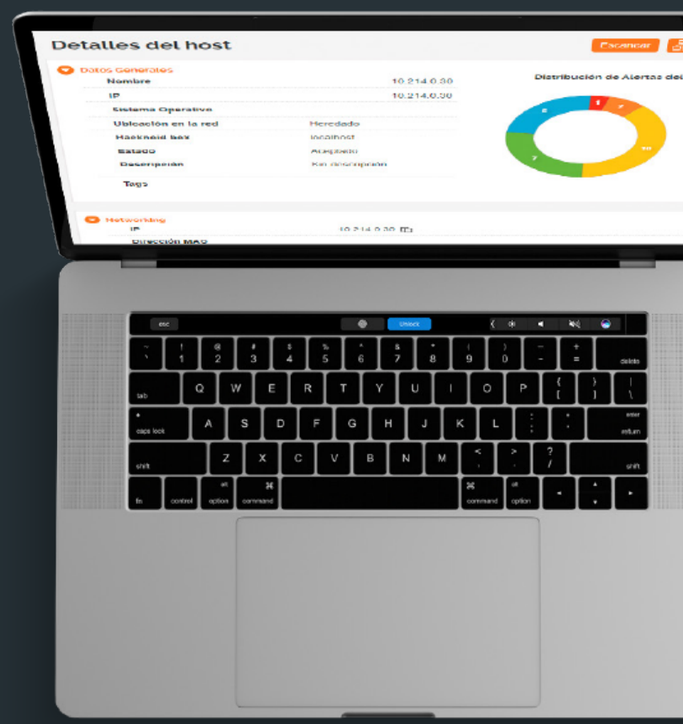
- Colores por criticidad
- Numeros de cantidad de alertas

25%

Los ciberataques a empresas crecen un 25% a causa de la pandemia.

80%

Casi el 80% de los líderes senior de TI y seguridad creen que sus organizaciones carecen de protección suficiente contra ciberataques.



Alertas

Clasificación por tipo de alerta y grado de criticidad, describe las características de la alerta y da detalles de soluciones.

Fuente de motores de búsqueda

Actualización automática.

CVE	Common vulnerabilities and exposures
CVSS	Common vulnerabilities scoring system
OWASP	Open Web Application Security Project

77%

Más del 77% de los afectados por ransomware estaban ejecutando una protección de endpoints actualizada

43%

El 43% de los ciberataques afectan a pequeños negocios.

Escaneo Web

Realiza un escaneo completo a tus aplicativos Web y sitios que expones a internet, realizando simulaciones de ataques dirigidos y fortuitos.

Hackeo Externo

Desde afuera de la organización, no solo pueden verse algunos aplicativos sino otros servicios que por razones de producción o muchas otras por descuidos dejan abiertas entradas de forma no segura permitiendo a cibercriminales obtener acceso, elevar privilegios para obtener accesos no deseados y lograr un sinfín de posibles ataques: es imprescindible tener nosotros mismos y lo antes posible, la visibilidad de como estamos expuestos hacia el mundo de internet para abordar la problemática y mitigar los riesgos a tiempo.

63%

El 63% de las empresas creen que los ciberataques han aumentado desde el año 2020 debido a la pandemia de COVID-19.

50%

La pérdida monetaria a causa del cibercrimen es de aproximadamente $945 mil millones de dólares en 2020, más del 50% de aumento en dos años.

COINTIC

Agenda

- Automaticos o a demanda
- Flexibles
- Granulares

Frecuencia de escaneo

Se pueden determinar frecuencias diferentes de escaneo para distintos grupos de activos o segmentos de red, según la criticidad de los mismos, la exposición, o cualquier criterio de negocio que se escoja tan granular como se desee.

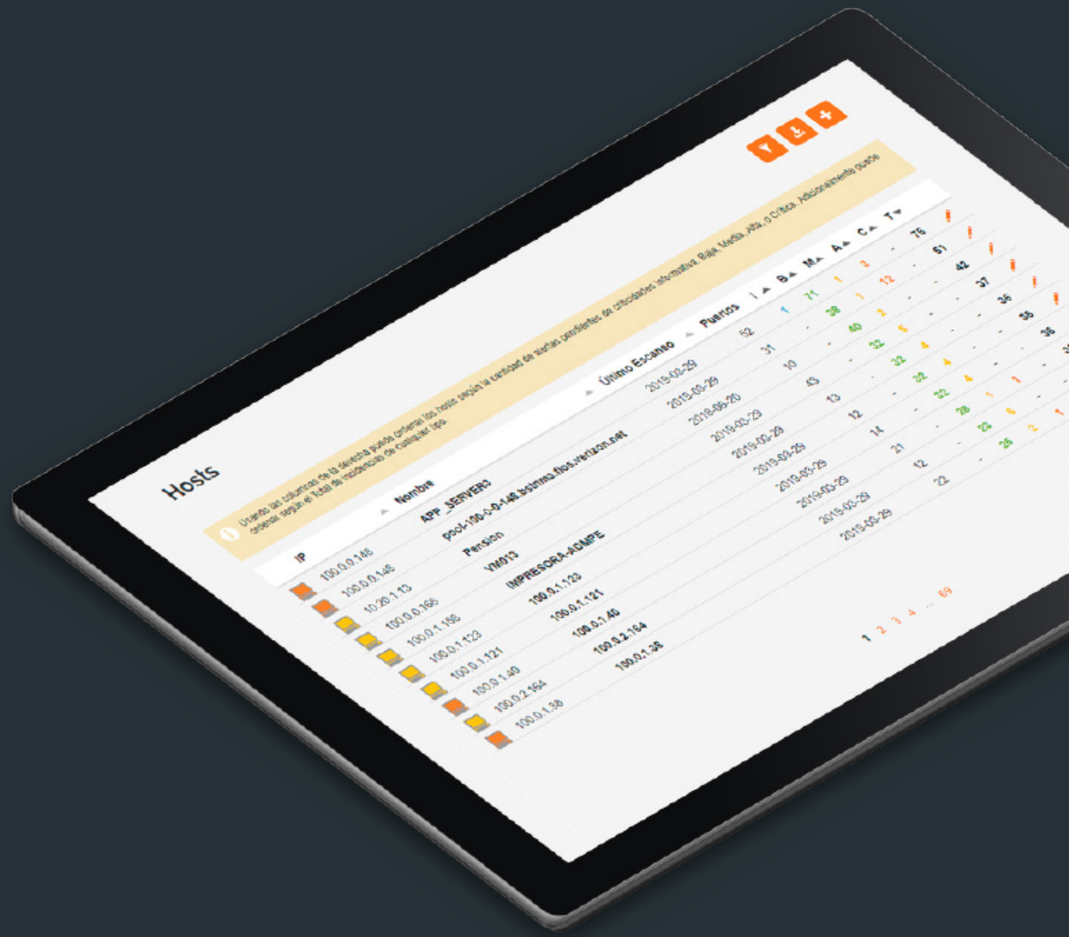
Liberar de este tiempo de ejecución, automatizando esta agenda, permite ganar tiempo de los recusos del equipo para resolver los operativos del día a día.

90%

Más del 90 por ciento de organizaciones de salud han reportado al menos una brecha de ciberseguridad en los últimos tres años.

93%

93% del malware observado el año 2019 es polimórfico, es decir que es capaz de modificar su programación para evitar ser detectado.



Reportes

- Analisis de vulnerabilidades
- Ethical Hacking
- Evolutivo
- Estadísticas
- PCI DSS
- ISO 27002
- NIST
- FISMA
- OWASP

En los reportes se exponen las alertas que levanta el escaneo continnuo en diversos formatos según distintas normativas para alinearse s los diferentes cumplimientos y marcos que requieran en la roganizacion.

Todas las alertas contienen un detallado nivel de descripcion de la misma, ubicación, categorizacion, identificacion y propuesta de solucion o guia.

Todos los reportes pueden ser completamente navegables y exportados en PDF o CSV.

86%

El 86 por ciento de las brechas de seguridad tienen una motivación financiera.

75%

75% de las organizaciones infectadas con ransomware tenían protección activa.

ALGUNOS CLIENTES **HACKNOID**

HACKNOID

SOLICITA UNA DEMO

www.cointic.com.mx

URUGUAY
Durazno 1504 Oficina 1 esq. Martínez Trueba
Palermo, Montevideo

CHILE
Av. Nueva Tajamar 481 Torre Norte, Of 1403,
Las Condes, Santiago

COINTIC

Av. Baja California No.245-piso
11 oficina 1101, Hipódromo,
Cuauhtémoc, 06170 Ciudad de México,
CDMX