HACKNOID

24/7 Vulnerability Analysis and Management

Your entire IT environment automatically monitored

www.hacknoid.com

What is Hacknoid?

Hacknoid is the only platform that gives visibility and comprehensively prioritizes your vulnerabilities.

We support your role as CISO by automating the search and continuous management of vulnerabilities in your technology environment, allowing you to address risk in a practical, simple and preventive way.

THE **IMPACT** BEFORE THE **FINANCIAL** AND **IMAGE** ATTACKERS IS INCONCEIVABLE

Find your vulnerabilities before attackers do

24X7 AUTOMATED

The most efficient way to protect your company against cyber-attacks is by fully automating vulnerability scanning and management every day of the year

ON-PREMISE CONFIGURATION, CLOUD, OR HYBRID ENVIRONMENTS

On-premise, cloud or hybrid environments will always be prone to certain risks that need to be protected against, with proper planning and configuration

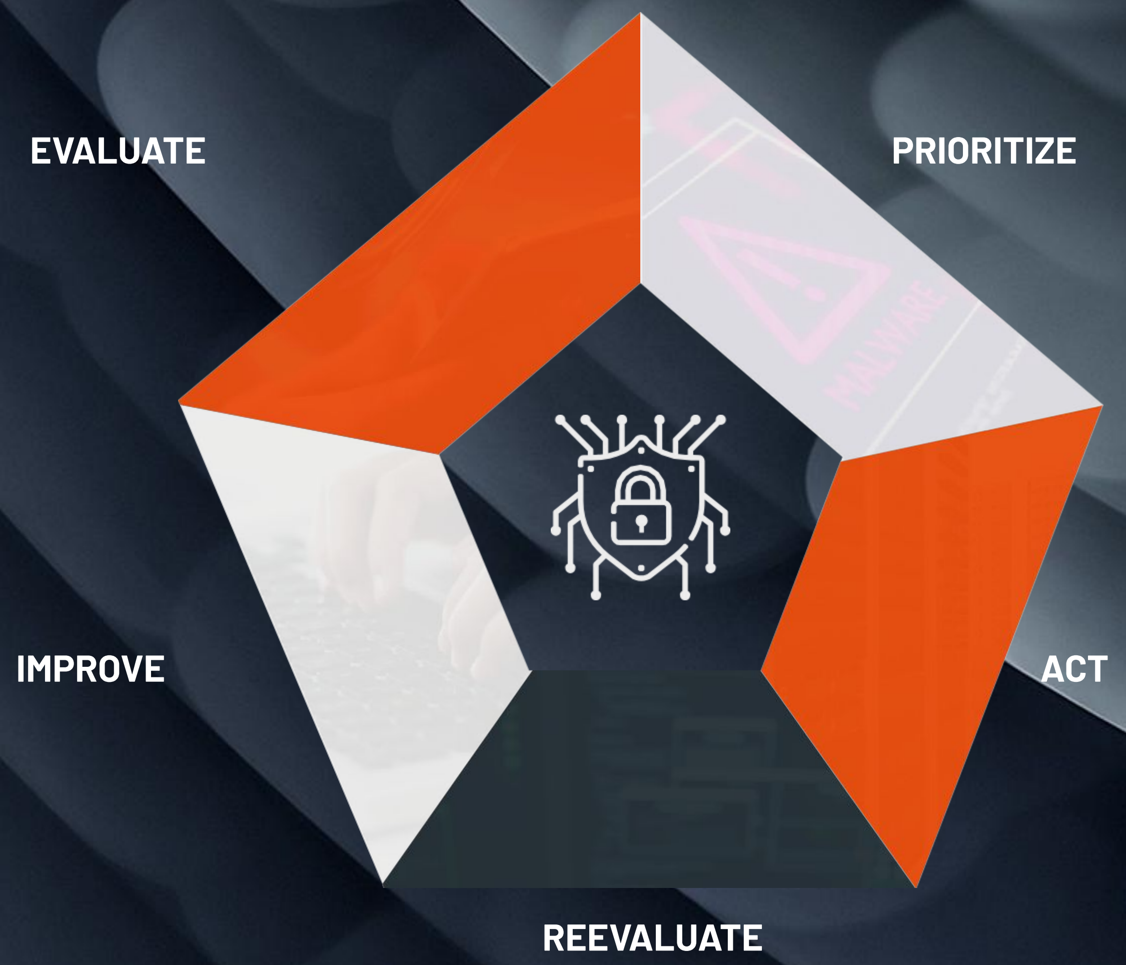
EASY AND SIMPLE GRAPHIC INTERFACE

Intuitive user interface allows you to being working, sprint, and manage risks accordingly.

Vulnerability Management Cycle

Previous Work

- Determine program scope
- Define roles and responsibilities
- Select scanning tools
- Create and refine policies and SLAs
- Identify sources of asset context



EVALUATE

PRIORITIZE

ACT

REEVALUATE

IMPROVE

HACKNOID REDUCES **CIBERSECURITY** OPERATIONAL WORKLOAD BY ALLOWING **FOCUSED EFFORTS**

Hacknoid Features

FUNCTIONAL

90%

90% of companies need more time or human resources.

SIMPLE

58%

58% of person-hours SAVED by the automation that can be derived for the execution of remediation.

CONTINUOUS

45%

45% of EFFORT is lost today on vulnerabilities with low exploitability due to an incorrect prioritization process.

Hacknoid Features

AUTOMATING VULNERABILITY TESTING

Organizations can significantly improve their security by implementing an automation platform that scans in 24/7 mode, the entire environment for vulnerabilities and other risk-associated issues.

Functional

Automates vulnerability scanning for the entire IT environment in a comprehensive, 24/7 mode.

Do you find it complex to deal with technology risk management?

We will take care of it!

Hacknoid Features

SIMPLE OVERVIEW OF CYBERSECURITY STATUS

Now your cybersecurity and IT team can have a single view of the security status of the entire environment, avoiding false positives and without tedious reporting.

The dashboard, which shows technicians and managers the state of health of cybersecurity in a simple way, with groupings and colors, allows you to identify points of higher criticality to order remediation quickly.

Simple

Visualize the security status of your entire technological infrastructure through a simple dashboard for both technicians and managers.

Lead your Cybersecurity Management

Request a Demo!

Hacknoid Features

CONTINUOUS VULNERABILITY ASSESSMENT

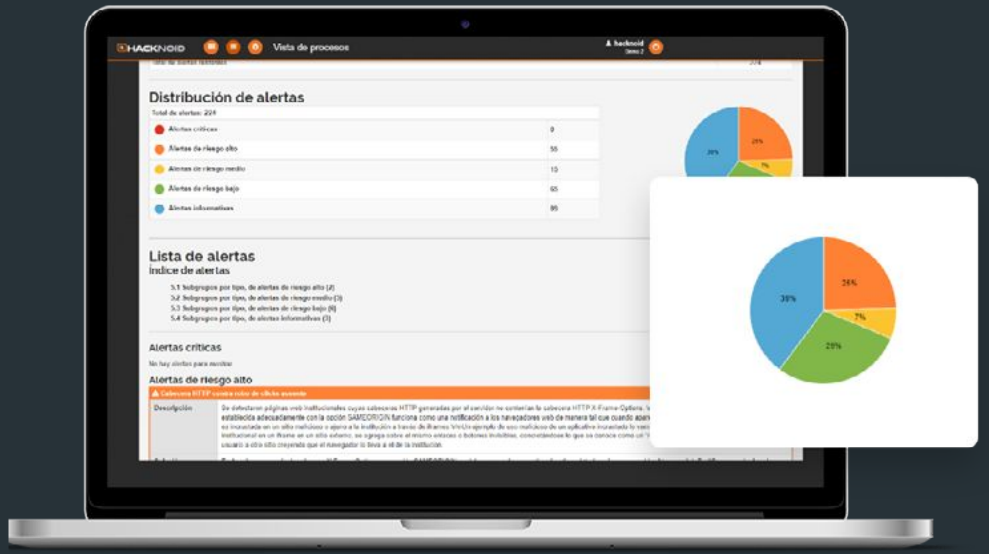
Vulnerabilities are reduced by being permanently alert and dealing with them continuously, ensuring that the time spent living with them is as short as possible. This provides the fundamental basis for business continuity, to act proactively and avoid affecting critical processes.

Continuous

Being permanently alert reduces the time of coexistence with vulnerabilities, avoiding system crashes or critical moments.

Minimize exposure times

Automate Cybersecurity



Distribución de alertas

Total de alertas: 224

● Alertas críticas	0
● Alertas de riesgo alto	58
● Alertas de riesgo medio	15
● Alertas de riesgo bajo	65
● Alertas informativas	86

Lista de alertas

Índice de alertas

5.1 Subgrupos por tipo, de alertas de riesgo alto (2)
5.2 Subgrupos por tipo, de alertas de riesgo medio (3)
5.3 Subgrupos por tipo, de alertas de riesgo bajo (8)
5.4 Subgrupos por tipo, de alertas informativas (3)

Alertas críticas

No hay alertas para mostrar

Alertas de riesgo alto

⚠ Cabecera HTTP contra robo de clicks ausente

Descripción: Se detectaron páginas web institucionales cuyas cabeceras HTTP generadas por el servidor no contenían la cabecera HTTP X-Frame-Options. [illegible] establecida adecuadamente con la opción SAMEORIGIN funciona como una notificación a los navegadores web de manera tal que cuando apar[illegible] es incrustada en un sitio malicioso o ajeno a la institución a través de iframes [illegible] Un ejemplo de uso malicioso de un aplicativo incrustado [illegible] institucional en un iframe en un sitio externo, se agrega sobre el mismo enlaces o botones invisibles, consiguiendo lo que se conoce como [illegible] usuario a otro sitio creyendo que el navegador lo lleva a él de la institución.

Dashboard

Enables comprehensive visibility of what is happening in security issues, immediately.

Widget

- Configurable by user and role
- Flexible grouping of assets according to criticality, location, or chosen criteria
- Flexible monitoring with granular and flexible frequencies also according to business criteria

Indicators

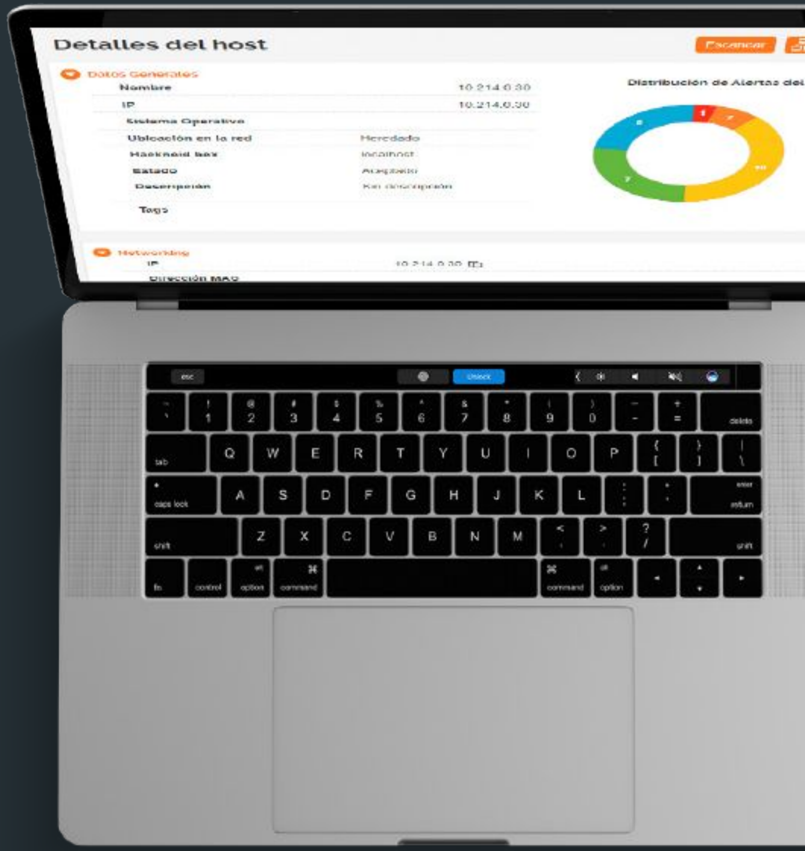
- Colors by criticality
- Alert quantity numbers

25%

Cyber-attacks on companies grow by 25% due to the pandemic.

80%

Nearly 80% of senior IT and security leaders believe their organizations lack sufficient protection against cyberattacks.


Detalles del host

Datos Generales

Nombre 10.214.0.30

IP 10.214.0.30

Sistema Operativo

Ubicación en la red Heredado

Hacknoid box localhost

Estado Aceptado

Descripción Sin descripción

Tags

Networking

IP 10.214.0.30

Dirección MAC

Alerts

Classification by type of alert and degree of criticality, describing the characteristics of the alert and giving details of solutions.

Search engine source

Automatic update.

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

77%

More than 77% of those affected by ransomware were running up-to-date endpoint protection.

43%

43% of cyberattacks affect small businesses.

Web Scanning

Performs a complete scan of your Web applications and sites that you expose to the Internet, simulating targeted and random attacks.

External Hacking

From outside the organization, not only some applications can be seen, but also other services that, for production reasons or many others due to carelessness, leave open entries in an unsecured way, allowing cybercriminals to gain access, elevate privileges to obtain an unwanted permits and achieve a variety of possible attacks: it is essential to have ourselves and as soon as possible, the visibility of how we are exposed to the Internet world to address the problem and mitigate the risks in time.

63%

63% of companies believe that cyber attacks have increased since 2020 due to the COVID-19 pandemic.

50%

The monetary loss from cybercrime was approximately $945 billion in 2020, a more than 50% increase in two years.

Agenda

- Automatic or on demand
- Flexible
- Granular

Scanning frequency

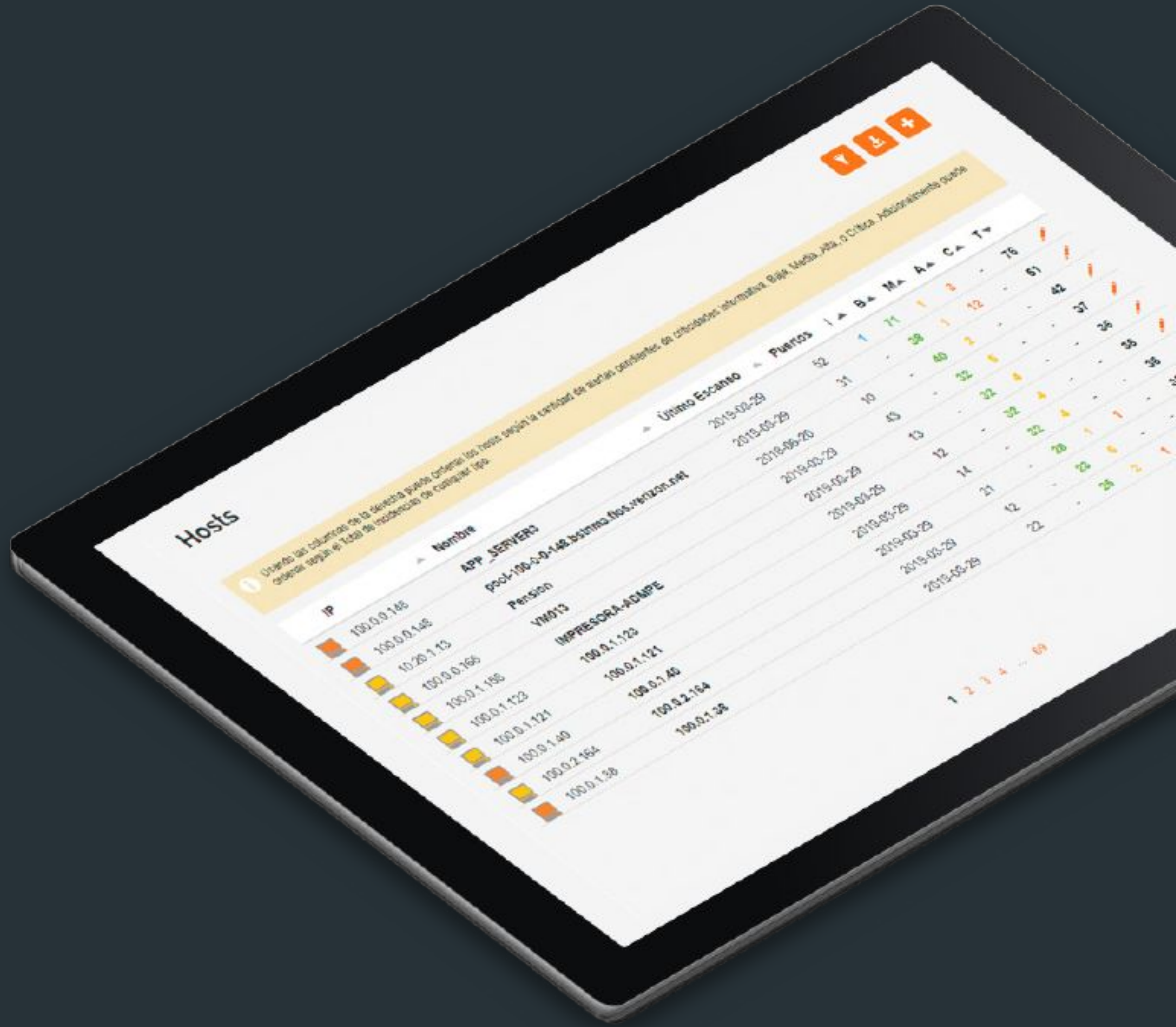
Different scanning frequencies can be determined for various asset groups or network segments, depending on asset criticality, exposure, or any business criteria you choose, as granular as desired.

90%

More than 90 percent of healthcare organization s have reported at least one cybersecurit y breach in the past three years.

93%

Ninety-three percent of malware observed in 2019 is polymorphic, meaning it can modify its programming to avoid detection.



Hosts

Usando las columnas de la derecha puede ordenar los hosts según la cantidad de alertas pendientes de criticidades informativa, Baja, Media, Alta, o Crítica. Adicionalmente puede ordenar según el Total de incidencias de cualquier tipo.

IP	Nombre	Último Escaneo	Puertos	I	B	M	A	C	T
100.0.0.148	APP_SERVER3	2019-02-29	52	1	11	1	3	-	76
100.0.0.146	pool-100-0-0-148.bstrmo.fios.verizon.net	2019-03-29	31	-	38	1	12	-	61
10.20.1.13	Pension	2018-06-20	10	-	40	3	-	-	42
100.0.0.166	VM013	2019-03-29	43	-	32	6	-	-	37
100.0.1.156	IMPRESORA-ADMPE	2019-03-29	13	-	32	4	-	-	36
100.0.1.123	100.0.1.123	2019-03-29	12	-	32	4	-	-	35
100.0.1.121	100.0.1.121	2019-03-29	14	-	22	4	1	-	36
100.0.1.40	100.0.1.40	2019-03-29	21	-	26	1	-	-	[illegible]
100.0.2.164	100.0.2.164	2019-03-29	12	-	23	6	1	[illegible]	[illegible]
100.0.1.38	100.0.1.38	2019-03-29	22	-	24	2	[illegible]	[illegible]	[illegible]

1 2 3 4 ... 69

Reports

- Vulnerability Assesment
- Ethical Hacking
- Progress Report
- Statistics Report
- PCI DSS
- ISO 27002
- NIST
- FISMA
- OWASP

The reports expose the alerts raised by continuous scanning in various formats according to different regulations to align with the different compliances and frameworks required in the organization.

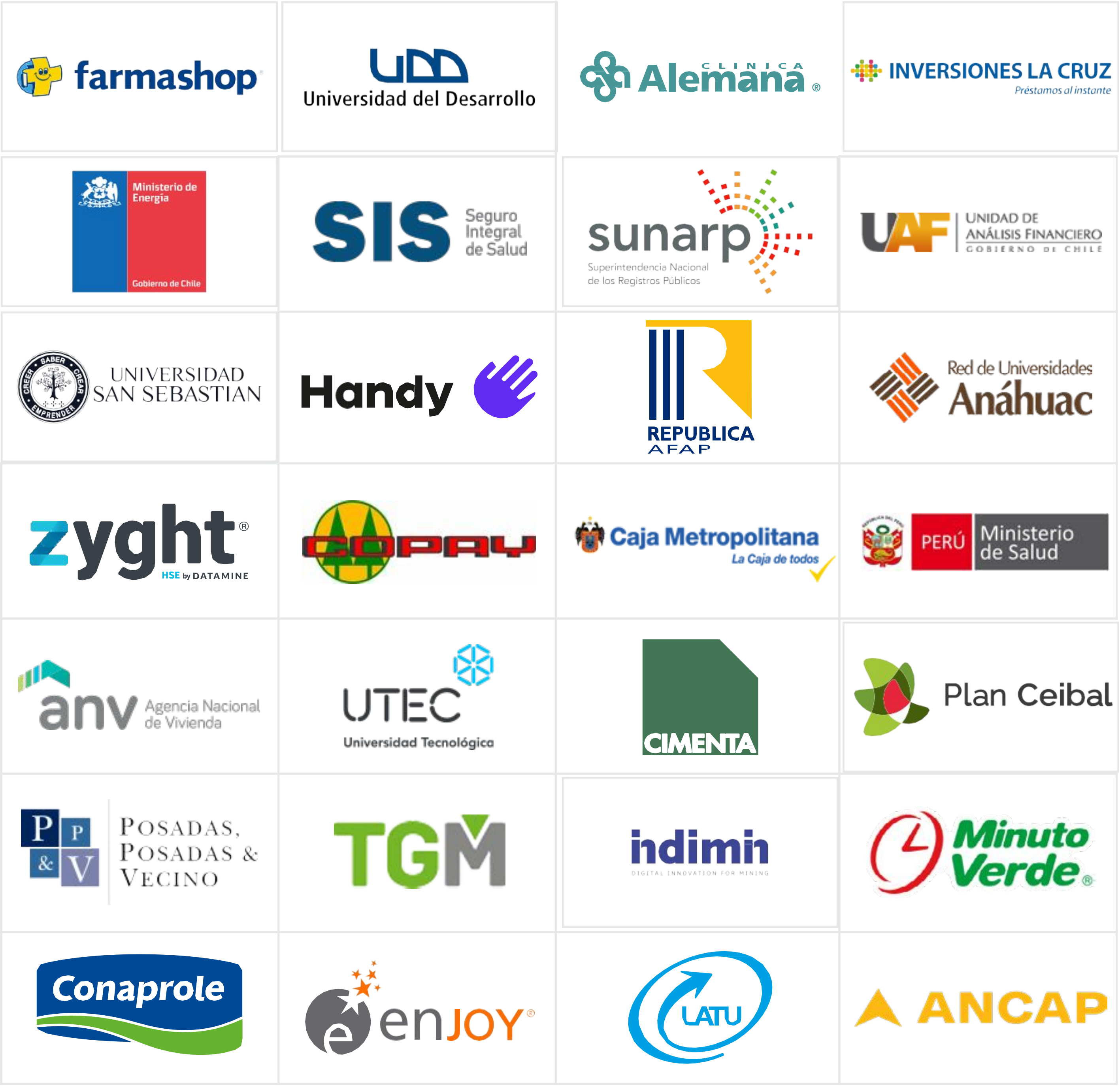
All alerts contain a detailed description of the alert, location, categorization, identification and proposed solution or guidance.

All reports can be fully navigable and exported in PDF or CSV.

86%
86 percent of security breaches are financially motivated.

75%
Seventy-five percent of organizations infected with ransomware had active protection.

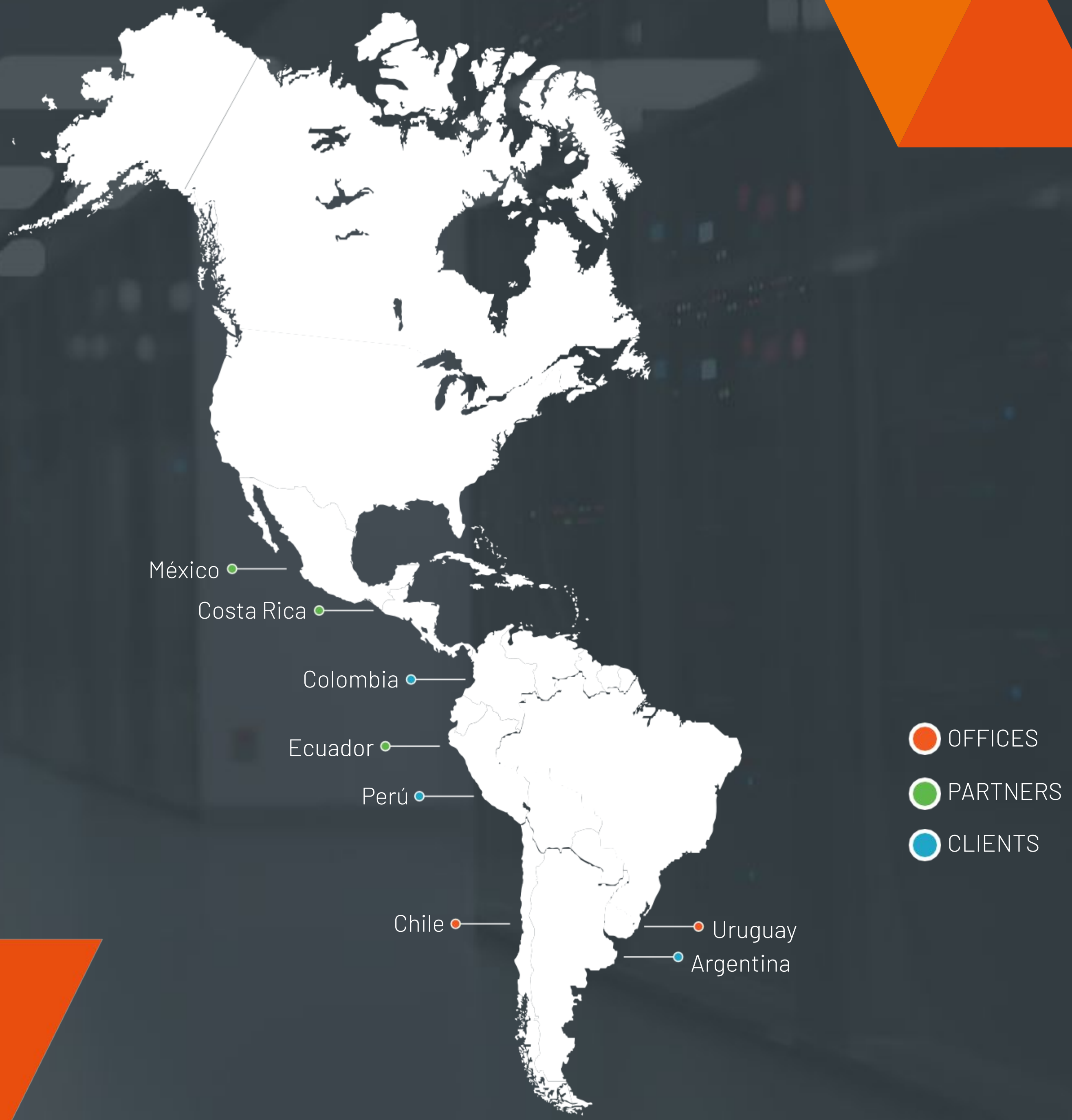
SOME
HACKNOID
CLIENTS



HACKNOID

REQUEST A DEMO

www.hacknoid.com



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

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