IXSY

Internet Exchange Services Yucatán A.C.

Juntos transformemos Yucatán
GOBIERNO DEL ESTADO

AYUNTAMIENTO DE MÉRIDA

INSTITUTO TECNOLÓGICO MÉRIDA YUCATÁN

RAM

AiTeLecom
INNOVATIVE COMMUNICATIONS

TRUXGO

MiOTT

BIGNET WIFI
Siempre Conectados!

TeleCable Yucatán

Totalplay
EMPRESARIAL

Internet Society

lacnic

ANUIES - TIC

SIIES
SECRETARÍA DE INVESTIGACIÓN, INNOVACIÓN Y EDUCACIÓN SUPERIOR 2018 - 2024

LAC-IX

NIC MÉXICO

canieti
SURESTE

socium
Su aliado seguro

MANRS

PROMTEL

ISP MX

Arelion

ufinet

aitdata
Servicios de Datacenter

anadic
yucatán

IENTC
TELECOMUNICACIONES

www.ixsy.org.mx

TRUXGO

- Empresa mexicana dedicada a la innovación e implementación de servicios en la nube para empresas, gobiernos y particulares.

- En los ultimos 7 años a desarrollado un equipo de seguridad informática evolucionandolo a CERT.

TRUXGO SECURITY

- Monitoreo y supervisión de red a más de 18 puntos de acceso alrededor del mundo, teniendo más de 17,000 servicios activos.

TRUXGO

Eventos al día

- 8,500,000 direcciones IP
- 750 TB de transferencia de datos

TRUXGO SECURITY

Eventos al día

- 75 eventos de DDoS
- 25 intentos de explotación de DB
- 1,000 intentos de intrusión
- 2,250,000 de correos spam

TRUXGO SECURITY

CERT TRUXGO

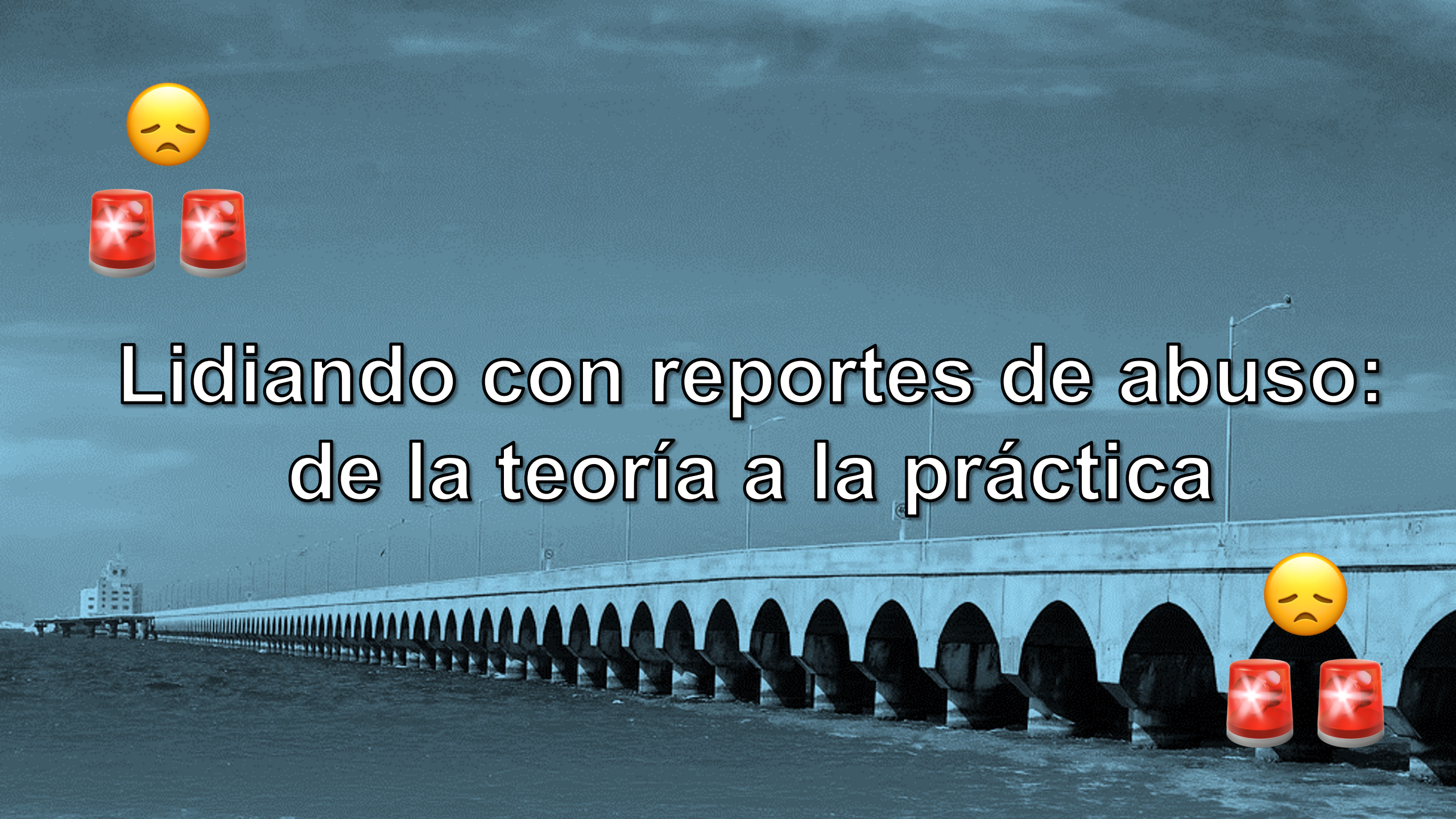
- Equipo Centralizado
- Modelo Híbrido
- Autoridad Total

TRUXGO SECURITY

Servicios del CERT

- Proteger y salvaguardar toda la infraestructura de TRUXGO y sus clientes.

TRUXGO SECURITY


Lidiando con reportes de abuso:
de la teoría a la práctica


SPAMHAUS


TALOS
CISCO


Barracuda


abusix


SpamRATS!
(Really Annoying Trouble Spots)


spamcop.net


CloudLock


AbuseIPDB


UCEPROTECT-NETWORK

Blacklisted

Reinicia el modem

[redacted] was found in our database!

This IP was reported **457** times. Confidence of Abuse is **100%**: ?

100%

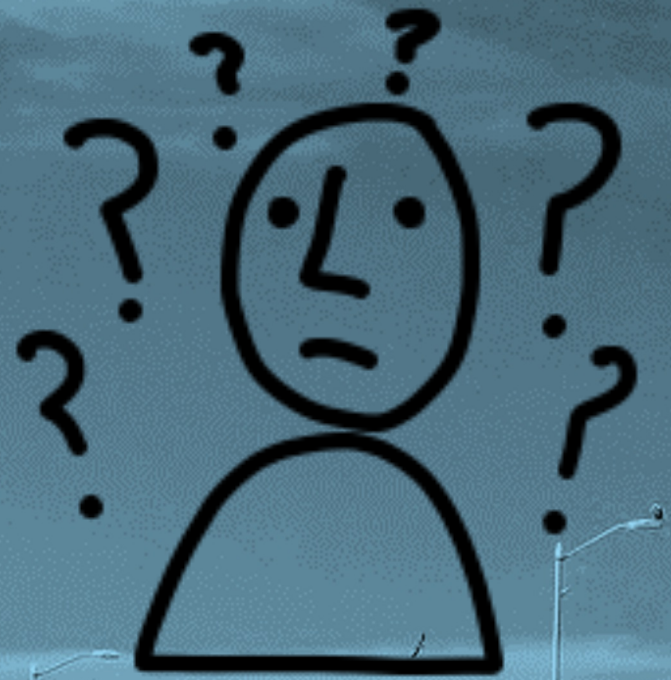
ISP	[redacted] Co. Ltd.
Usage Type	Search Engine Spider
Domain Name	[redacted]
Country	China
City	Beijing, Beijing

IP info including ISP, Usage Type, and Location provided by IP2Location. Updated monthly.

REPORT 180.76.104.41 WHOIS 180.76.104.41

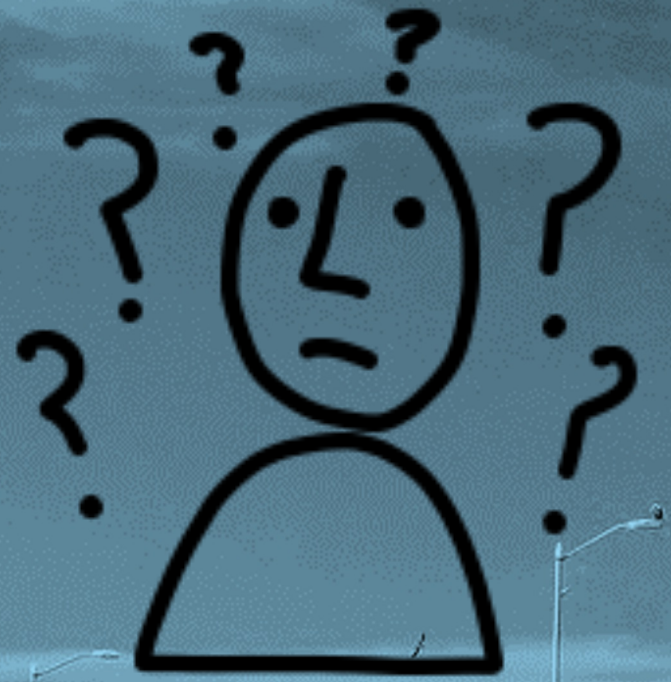
Reporter	Date	Comment	Categories
✔ 1000grad.com	1 minute ago	5x Failed Password	Brute-Force SSH
✔ woutvde	5 hours ago		Brute-Force SSH
✔ InfinitzHost	5 hours ago	Unauthorized connection attempt detected from IP add ress [redacted] to port 22 [V]	Brute-Force Exploited Host
✔ HyperSpeed	5 hours ago	Jul 4 13:17:02 NY2 sshd[3129620]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid= ... show more	Brute-Force SSH
✔ Parth Maniar	5 hours ago	SSH login attempts (SSH bruteforce attack). For more i nformation, or to report interesting/incorrect ... show more	Brute-Force SSH
✔ AdrianT	13 hours ago	SSH brute force	Brute-Force SSH
✔ ZeroAttackVector	14 hours ago	zrh: 3 unauthorised SSH/Telnet login attempts between 2022-07-04T03:50:20Z and 2022-07-04T03:57:29Z	Brute-Force SSH
✔ M127	14 hours ago	Jul 4 03:49:49 scw-tender-jepsen sshd[18272]: Failed p assword for root from [redacted]1 port 5892 ... show more	Brute-Force SSH

¿Qué es un reporte de abuse?



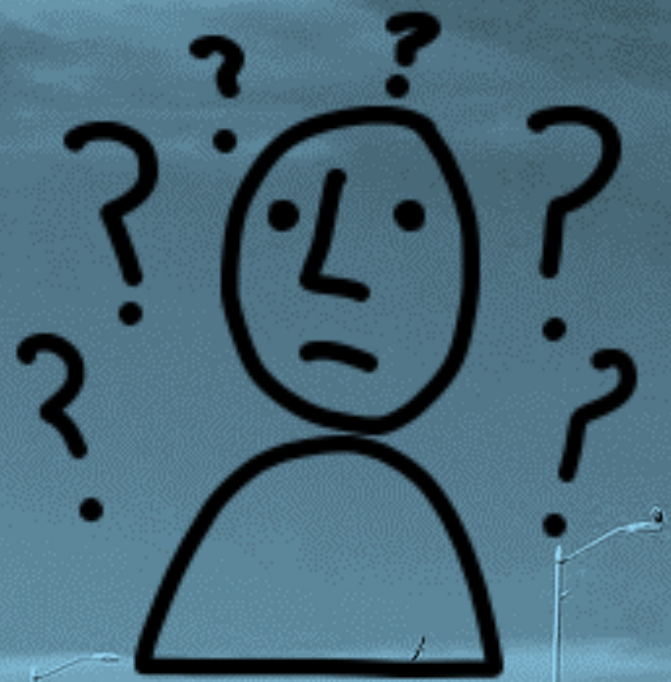
Es una solicitud en la cual se reporta una falta a las políticas de uso aceptable del servicio de internet, realizada por una dirección IP, domino web, servidor o servicio.

¿Por qué tengo reportes de abuse?



- Configuraciones erróneas
- Uso inadecuado de los recursos
- Reportes de la comunidad
- Falsos positivos

Causas frecuentes



- SPAM
- DDOS
- Phishing
- Port Scaning
- Virus / Malware
- Configuraciones erróneas
- Copyright


Acciones
preventivas

¿Qué se debe de hacer?

Dar importancia al área y brindar presupuesto acorde a las necesidades

Facilitar otros medios de contacto

Integrar al centro de respuesta ante incidentes en los casos

¿Qué se debe de hacer?

Establecer políticas preventivas en la entrega de los servicios

Hacer monitoreo frecuente de los recursos.

Colaborar con el CSIRT-CERT

¿Qué se debe de hacer?

Especializar un departamento de ABUSE

Identificar el servicio que se le da a los recursos otorgados al usuario final

Coordinación directa ante eventos críticos

¿Qué se debe de hacer?

Identificar el uso que se le dará a los recursos

Notificar las políticas de uso aceptable

Coordinación directa ante eventos críticos


Acciones
correctivas

¿Qué se debe de hacer?

Tener un programa de soluciones críticas sobre recursos afectados

Facilitar los procesos y presupuestos ante el evento

Coordinar acciones con las áreas involucradas

¿Qué se debe de hacer?

Identificar causa y motivo del reporte

Verificar si se incumplieron políticas de entrega

Enviar evidencias al CSIRT-CERT

Contactar a la entidad del reporte y determinar acciones

¿Qué se debe de hacer?

Brindar protocolo de identificación

Comunicar el reporte a la área responsable

Brindar soluciones alternas al cliente

Dar comunicado final (positivo-negativo)


Soluciones
bases

Los recursos deben estar sub asignados

WHOIS

Domain or IP

WHOIS

Las direcciones deben contar con PRT

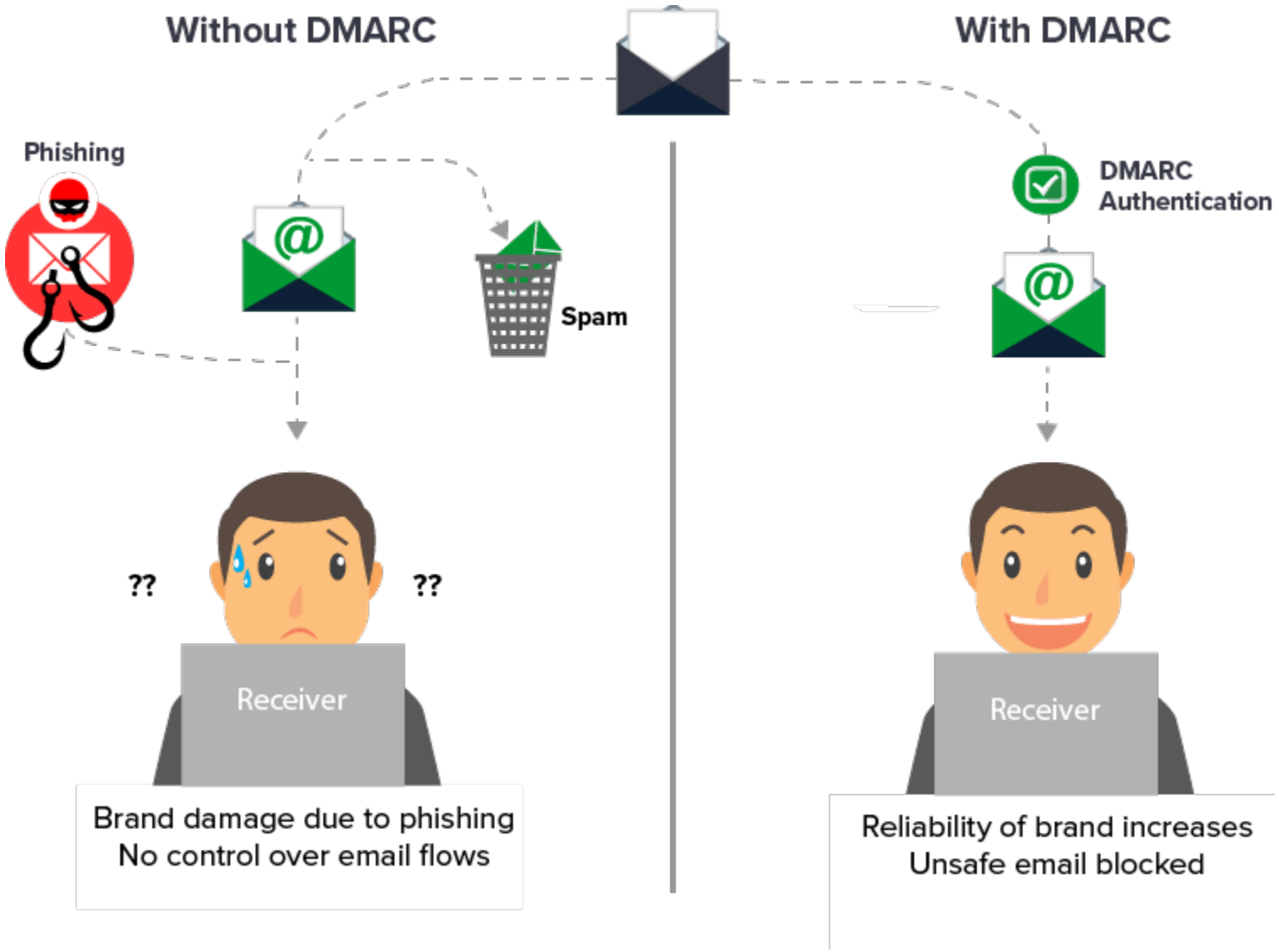
DNS Lookup (A Record)

truxgo.com → 131.196.253.94

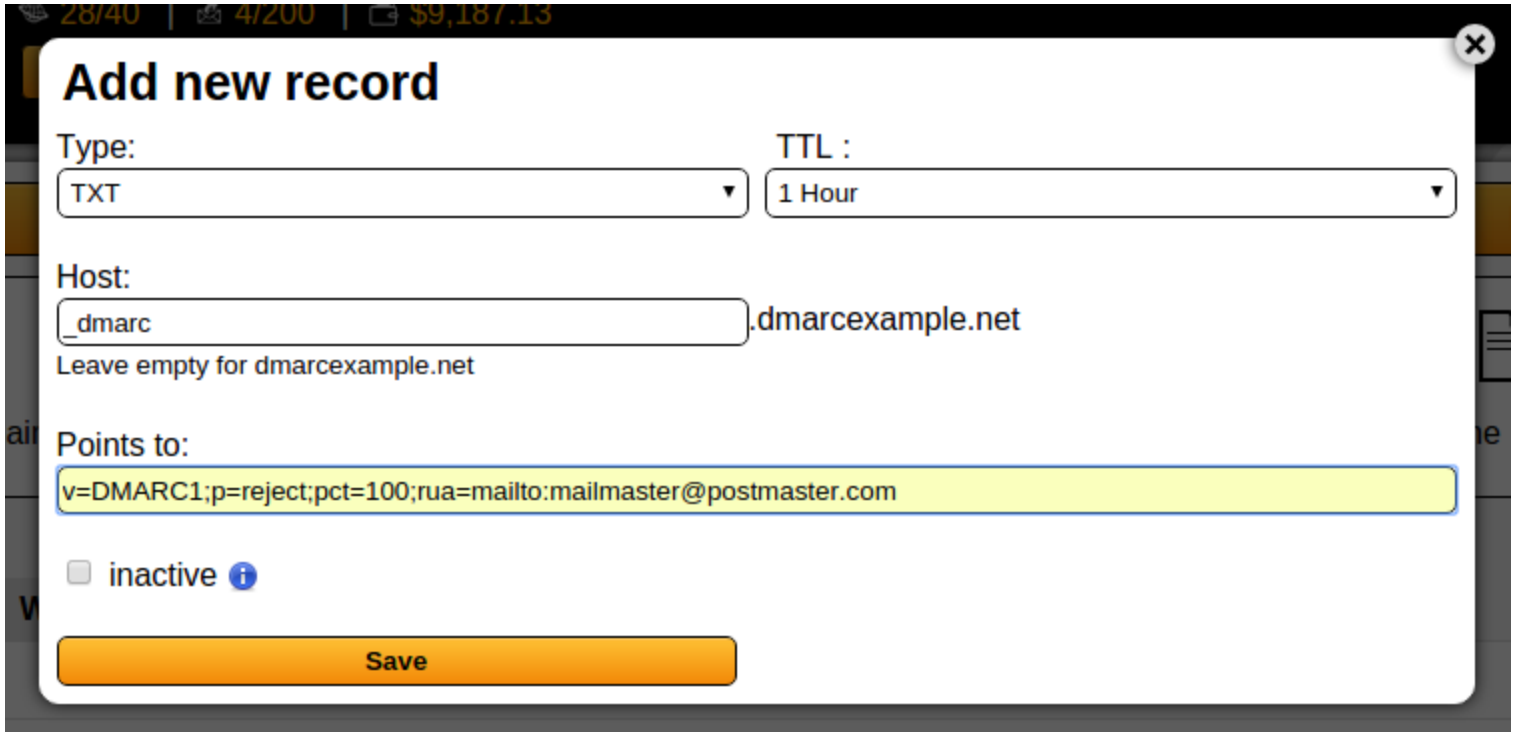
DNS Lookup (PTR Record – rDNS – Reverse DNS)

131.196.253.94 → truxgo.com

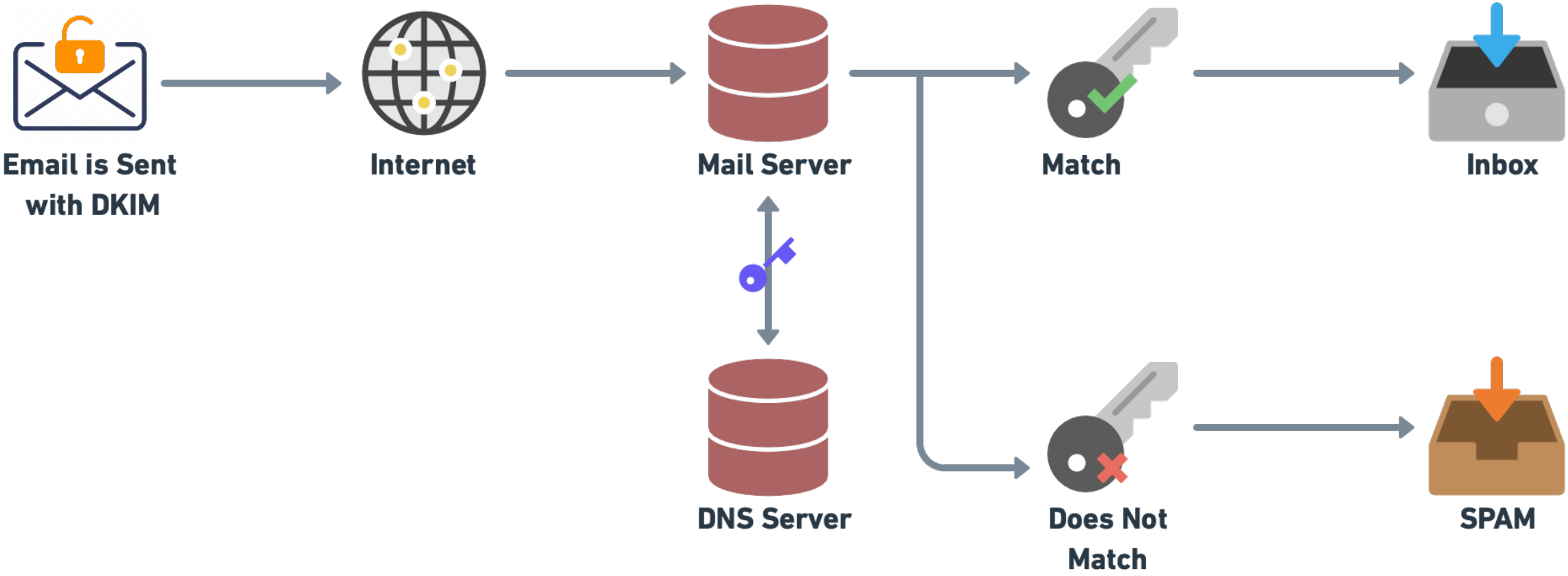
Deben contar con DMARC



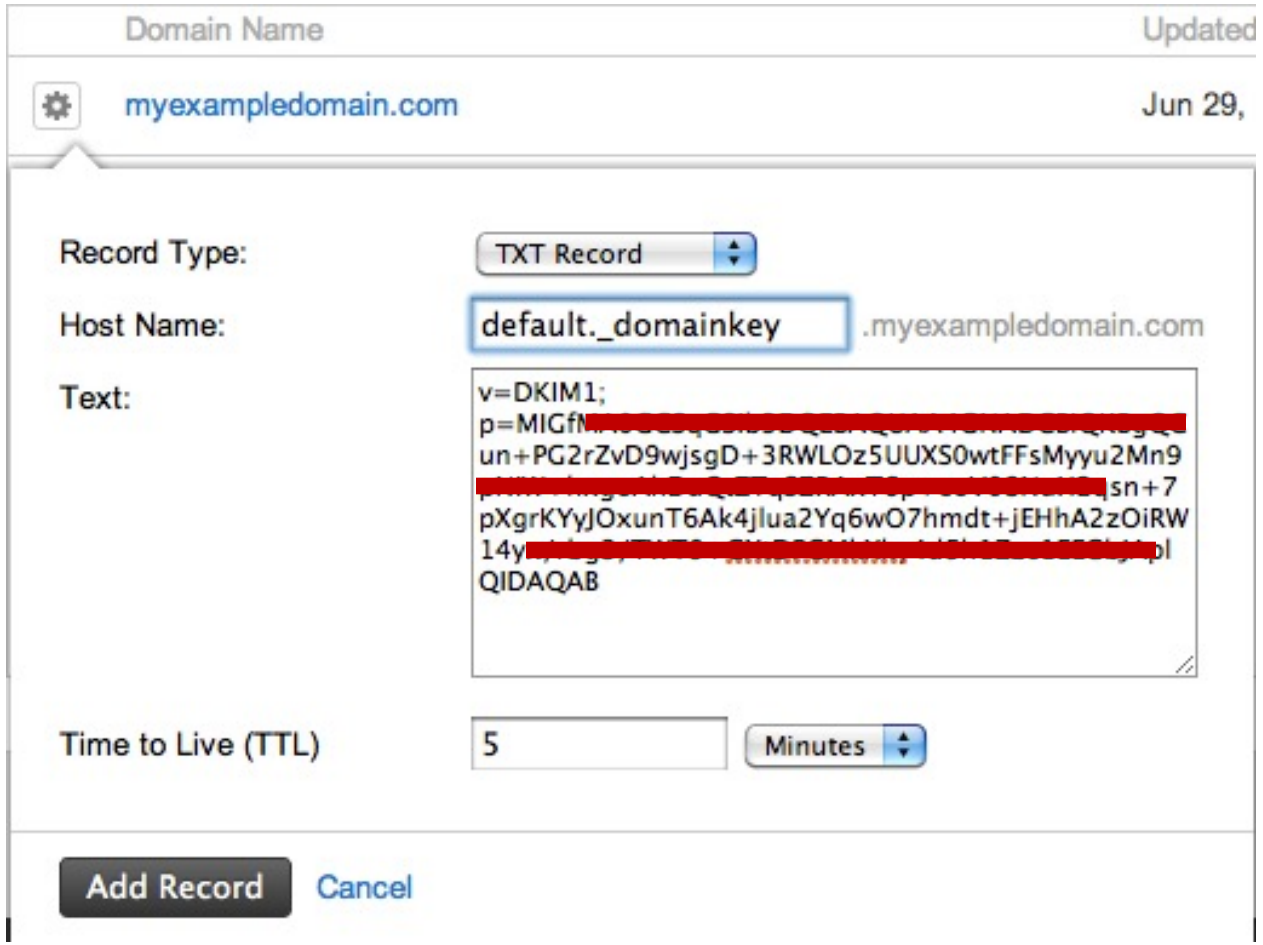
Deben contar con DMARC



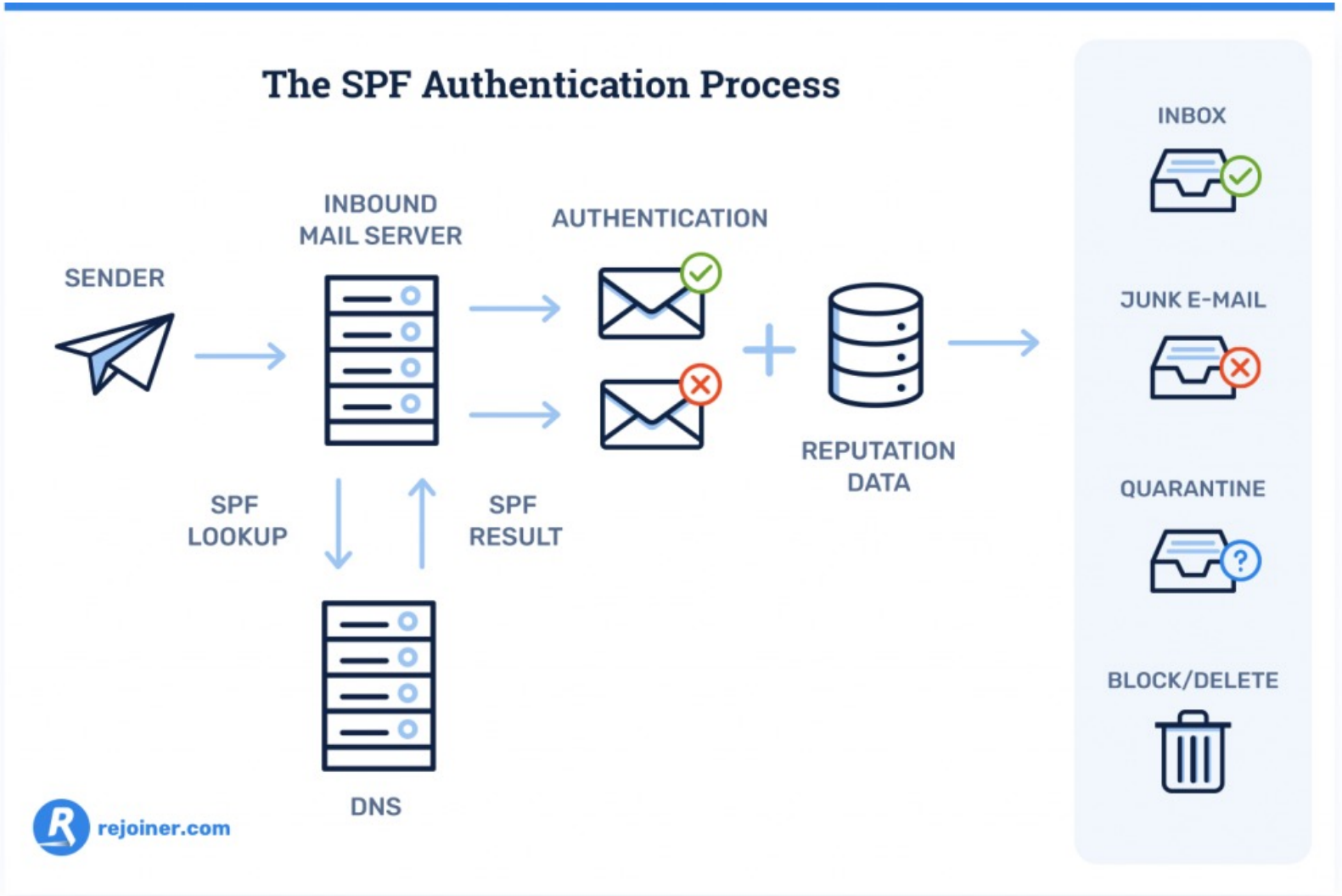
Deben contar con DKIM



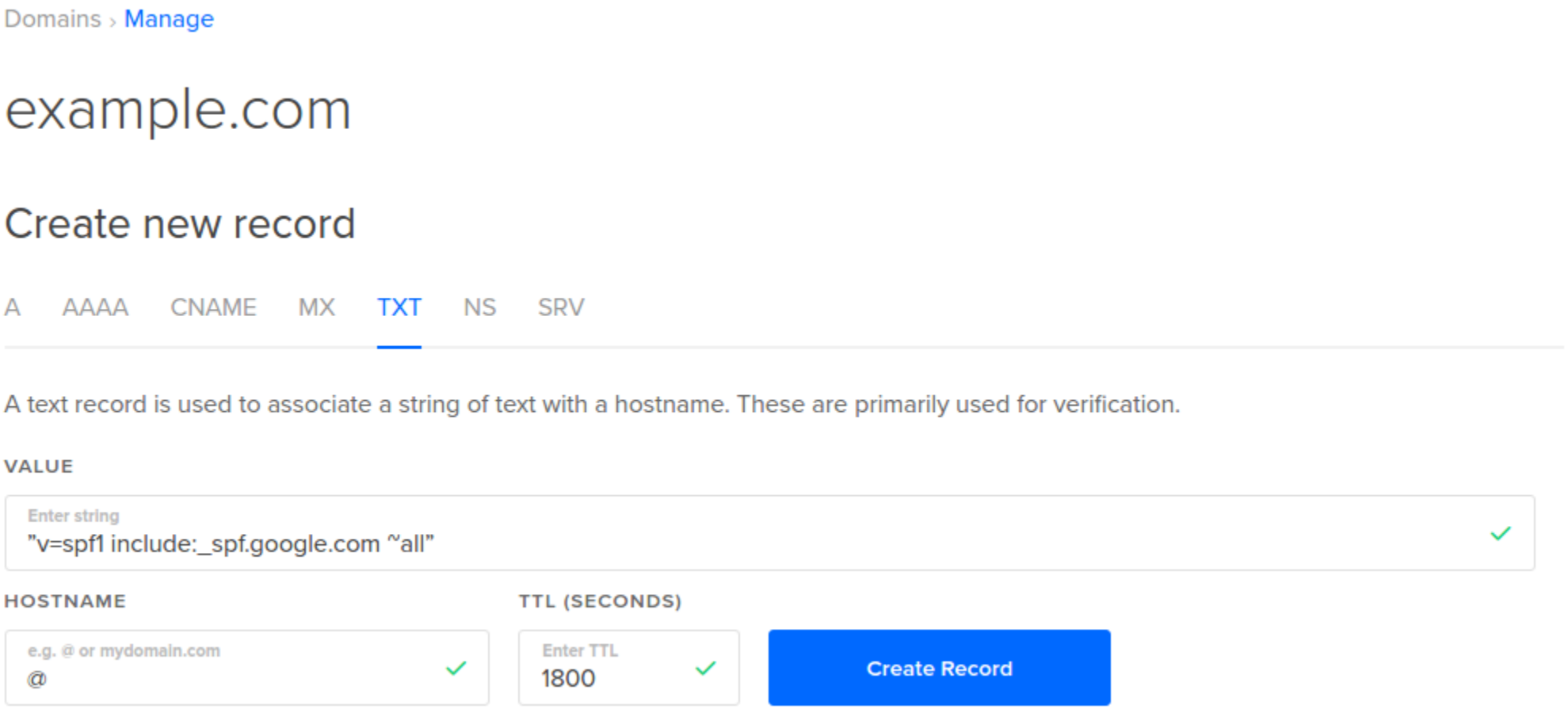
Deben contar con DKIM



Deben contar con SPF



Deben contar con SPF



Los 3 son necesarios

Servidor Autorizado

Contacto responsable

Llaves de identificación

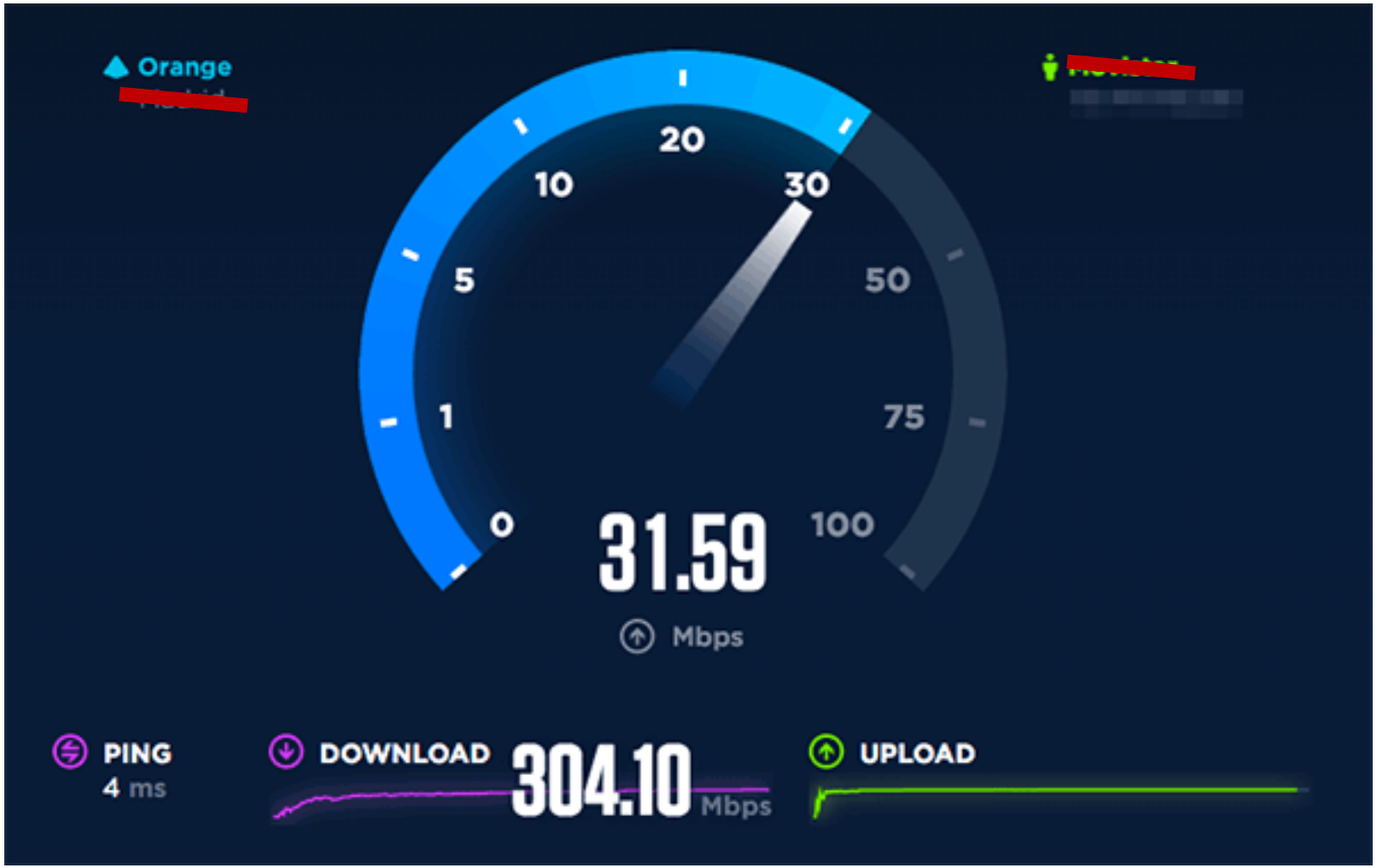
Bloqueo de Puertos

25

80

21

Limitar la transferencia de datos



Monitoreo de Infraestructura

Herramientas

MX TOOLBOX®

	Blacklist
OK	ivmURI
OK	Nordspam DBL
OK	SEM FRESH
OK	SEM URI
OK	SEM URIRED
OK	SORBS RHSBL BADCONF
OK	SORBS RHSBL NOMAIL
OK	Spamhaus DBL
OK	SURBL multi
OK	0SPAM
OK	Abuse.ro
OK	Abusix Mail Intelligence Blacklist
OK	Abusix Mail Intelligence Domain Blacklist
OK	Abusix Mail Intelligence Exploit list
OK	Anonmails DNSBL
OK	BACKSCATTERER
OK	BARRACUDA
OK	BLOCKLIST.DE
OK	CALIVENT
OK	CYMRU BOGONS
OK	DAN TOR

MX Lookup

Blacklists

DMARC

DNS Lookup

Email Health

Analyze Headers

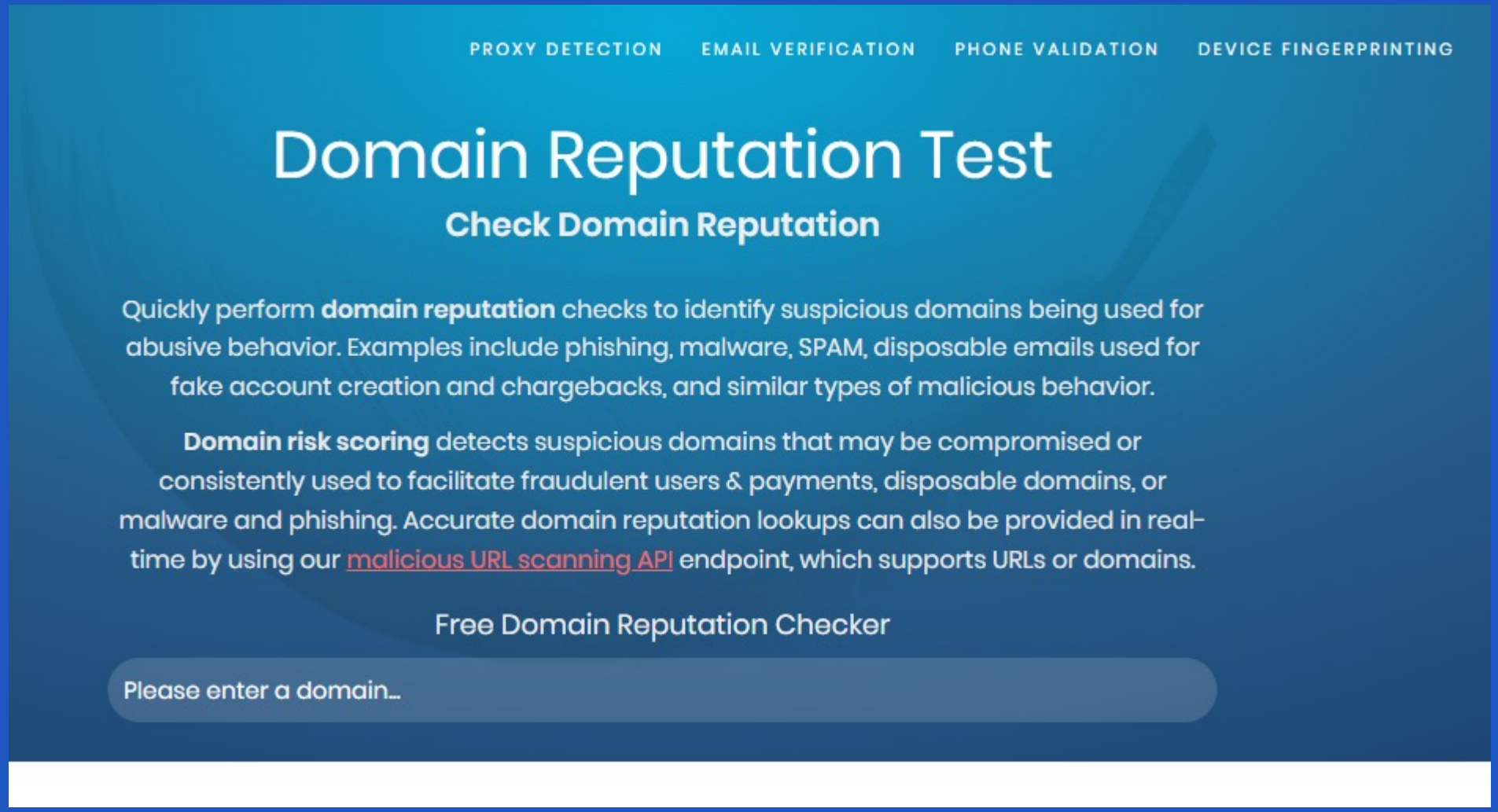
mail tester


Comprueba el grado de spam de tus correos
Primero, envía tu correo a:
test-owh1umufu@srv1.mail-tester.com
A continuación comprueba tu puntuación

CYREN


CYREN
Cyren stops phishing attacks
Cyren Inbox Security continuously monitors Microsoft 365 inboxes and automatically remediates advanced email phishing attacks that evade SEGs.
REQUEST A DEMO

IPQUALITYSCORE
PROACTIVELY PREVENT FRAUD™



IPVOID

Engine	Status
AZORult Tracker	✔
AntiSocial Blacklist	✔
Artists Against 419	✔
Badbitcoin	✔
Bambenek Consulting	✔
CERT Polska	✔
CERT-GIB	✔
CERT-PA	✔
CRDF	✔
C_APT_ure	✔
Chong Lua Dao	✔
CoinBlockerLists	✔
Cyber Threat Coalition	✔
CyberCrime	✔
EtherAddressLookup	✔
EtherScamDB	✔

IP TOOLS ▾ DNS TOOLS ▾

- IP BLACKLIST CHECK
- WHOIS LOOKUP
- IP GEOLOCATION
- IP TO COUNTRY NEW
- IP TO ASN NEW
- IP TO GOOGLE MAP
- IPV4 CIDR CALCULATOR NEW
- IPV4 CIDR CHECKER NEW
- IPV6 CIDR CALCULATOR NEW
- MY IP ADDRESS
- IP TO DECIMAL NEW
- PING LOOKUP
- IPV6 PING TEST NEW
- OPEN PORTS
- PORT SCANNER
- UDP PORT SCANNER NEW
- TRACEROUTE
- WEBSITE LOCATION NEW
- FIND WEBSITE IP
- EXTRACT IPS

DNS TOOLS ▾ TEXT TOO

- DIG DNS LOOKUP
- DNS REPUTATION NEW
- DNS PROPAGATION NEW
- MX LOOKUP
- REVERSE DNS LOOKUP
- NS LOOKUP
- DNSSEC LOOKUP
- DNSSEC VERIFIER NEW
- DNSKEY LOOKUP
- DMARC LOOKUP
- AAAA IPV6 LOOKUP
- TXT LOOKUP

URL TOOLS ▾ ENC/DEC TOOLS ▾

- HTTP/2 TEST
- TRACK HTTP REQUESTS NEW
- MULTI URL OPENER NEW
- SSL CERTIFICATE CHECK NEW
- DOMAIN REPUTATION CHECK NEW
- DOMAIN AGE CHECK NEW
- CAPTURE WEBSITE SCREENSHOT NEW
- HTTP RESPONSE HEADERS

McAfee

McAfee

McAfee Home ▸ Customer URL Ticketing System

Customer URL Ticketing System

Check Single URL

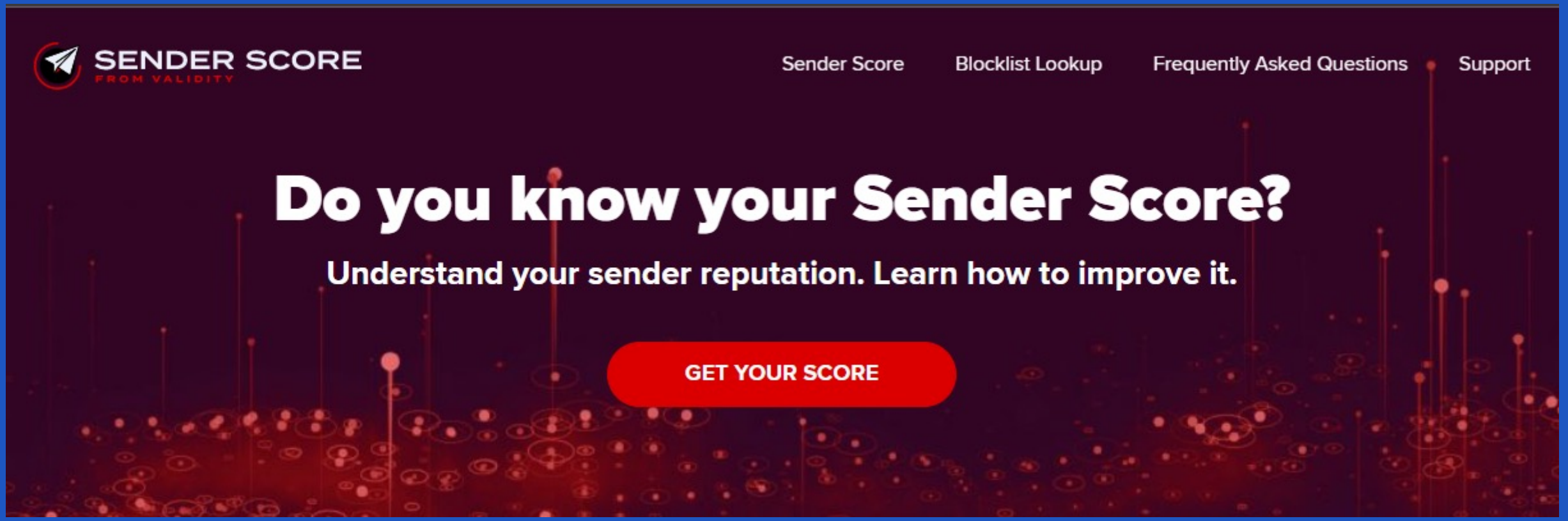
McAfee® provides an online tool that enables you to check if a site is categorized within various versions of the SmartFilter Internet Database or the Webwasher URL Filter Database. After you check a URL, this tool also allows you to suggest an alternative categorization for a site. These requests will be addressed within an average of 3-5 business days with some requests requiring additional review and taking longer.

Please select the product you are using. Selecting the appropriate product will provide the correct categorization information to be displayed for you.

-- Please Select --

-- Please Select --
McAfee Real-Time Database
McAfee SmartFilter XL
McAfee SmartFilter 4.2 (XL-1)
McAfee WebWasher 6.8.x
McAfee SiteAdvisor/Web Control (Enterprise)
McAfee SaaS Web Protection
McAfee Web Gateway v7.x/6.9.x (Cloud)
McAfee Web Gateway v7.x/6.9.x (Resident)


SENDER SCORE
FROM VALIDITY


SENDER SCORE
FROM VALIDITY
Sender Score
Blocklist Lookup
Frequently Asked Questions
Support
Do you know your Sender Score?
Understand your sender reputation. Learn how to improve it.
GET YOUR SCORE

EASYDMARC

DMARC

DMARC Lookup | DMARC Generator

DMARC Record Generator

Use this tool to generate your DMARC record

Domain

Policy type (None (monitoring) / Quarantine / Reject)

Reports send to (e.g. example@easydmarc.com)

Subdomain policy (----)

SPF identifier alignment (----)

DKIM identifier alignment (----)

Reporting interval

Percentage applied to (100)

Failure reporting send to (e.g. example@easydmarc.com)

Failure reporting options (0 / 1 / d / s)

Generate

Scanning results

No domain scanned

PROTECTION STATUS

0 of 10

No Data

Scan Domain →

DMARC — INVALID

SPF — INVALID

DKIM — INVALID

BIMI — INVALID

REPUTATION

Start Monitor

VIRUSTOTAL

VIRUSTOTAL

Analyze suspicious files, domains, IPs and URLs to detect malware and other breaches, automatically share them with the security community

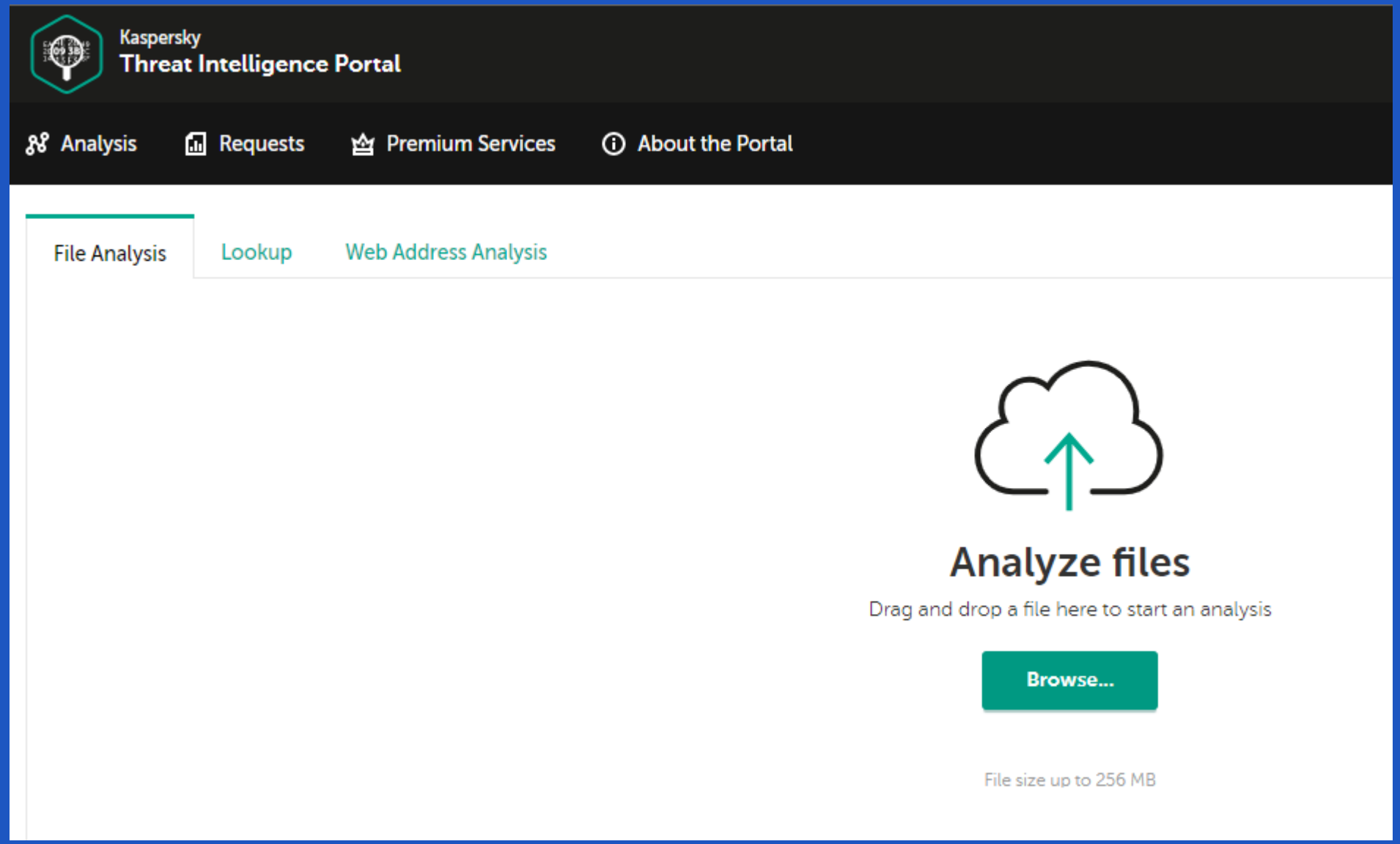
FILE | URL | SEARCH

Choose file

By submitting data above, you are agreeing to our Terms of Service and Privacy Policy, and to the **sharing of your Sample submission with the security community.** Please do not submit any personal information; VirusTotal is not responsible for the contents of your submission. Learn more.

ⓘ Want to automate submissions? Check our API, free quota grants available for new file uploads

Kaspersky
Threat Intelligence



OPSWAT.
MetaDefender


Soluciones
por organización

Dificultad: ★ ★ ★
Categorías: SBL / XBL / PBL / DBL / ZEN / CSS
Tiempo: Definido por las categorías

Especialidad: SPAM / Phishing
Reporta: IPv4 / IPv6 / ASN / Dominios
Bloqueo: Puede bloquear todo el prefijo asignado
Avisos previos: Definido por las categorías

Solución
PTR: Si DKIM: Si DMARC: Si
Justificación: Si
Bloqueo de puerto 25 : Definido por las categorías
Email del Whois: Si
Email test: Definido por las categorías

Barracuda

Dificultad: ★ ★ ★ ★
Categorías: General
Tiempo: 2 semanas – 2 meses

Especialidad: SPAM / Virus
Reporta: IPv4 / IPv6 / Dominios
Bloqueo: Puede bloquear todo el prefijo asignado
Avisos previos: Si

Solución
PTR: No DKIM: No DMARC: No
Justificación: Si
Bloqueo de puerto 25 : No
Email del Whois: Si
Email test: No

spamcop.net

Dificultad: ★
Categorías: BL Spamcop
Tiempo: Definido por categoría

Especialidad: SPAM
Reporta: IPv4 / IPv6 / Dominios
Bloqueo: Puede bloquear todo el prefijo asignado
Avisos previos: Si

Solución
PTR: Si DKIM: Si DMARC: Si
Justificación: No
Bloqueo de puerto 25 : Definido por las categorías
Email del Whois: Si
Email test: Definido por categoría

Dificultad: ★ ★ ★ ★ ★
Categorías: Spam / Hacking / Botnets / DDOS / Phishing
Tiempo: Definido por las categorías

Especialidad: Spam / Hacking / Botnets / DDOS / Phishing
Reporta: IPv4 / IPv6
Bloqueo: Puede bloquear desde una dirección IP
Avisos previos: No

Solución
PTR: No DKIM: No DMARC: No
Justificación: Si
Bloqueo de puerto 25 : No
Email del Whois: Si
Email test: No

SpamRATS!
(Really Annoying Trouble Spots)

Dificultad: ★ ★ ★ ★ ★
Categorías: RatsDYNA / RatsnoPTR / RatsSPAM/ RatsnoAuth
Tiempo: Definido por las categorías

Especialidad: SPAM
Reporta: IPv4 / IPv6 / ASN / Dominios
Bloqueo: Puede bloquear todo el prefijo asignado
Avisos previos: No

Solución
PTR: Si DKIM: Si DMARC: Si
Justificación: Si
Bloqueo de puerto 25 : Definido por las categorías
Email del Whois: Si
Email test: Definido por las categorías

Gracias

Jorge Varela

TRUXGO

IXSY
Internet Exchange Services Yucatán A.C.

Contacto

Email: varela_george@corp.truxgo.com

Cel: 2223216515

soyjorgevarela