

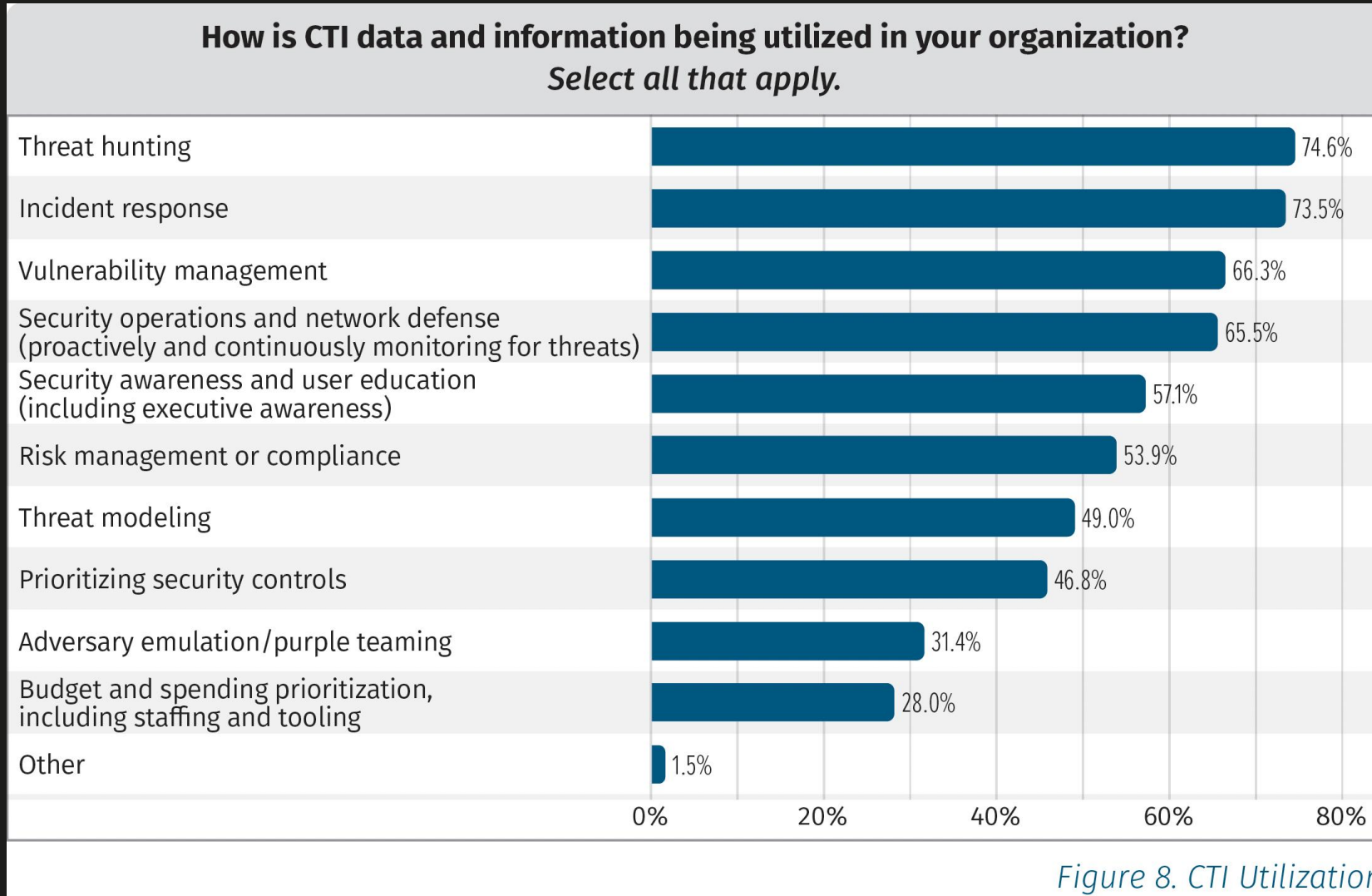
# Kaspersky Data Feeds for Firewalls



Pedro Jorge Viana de Bragança  
Head of Presales  
Spain and Portugal

**“La inteligencia sobre amenazas cibernéticas consiste en saber qué hacen tus adversarios y usar esa información para mejorar la toma de decisiones.”**

**MITRE**



Fonte: SANS CTI Survey 2024: Managing the Evolving Threat Landscape.

## INFORME SANS 2024

Una de las principales conclusiones destacadas por el informe es significativa y resalta el valor de la inteligencia de amenazas.

Por primera vez en la historia de la investigación, la caza de amenazas es el principal caso de uso para la inteligencia de amenazas cibernéticas (CTI).

Una caza de amenazas eficaz depende en gran medida de feeds de datos de amenazas de red (Network Threat Data Feeds) de alta calidad.

Estos feeds proporcionan información actualizada y relevante sobre comportamientos maliciosos, indicadores de compromiso (IoCs) y técnicas utilizadas por los adversarios.,.

# Inteligencia de Amenazas – ¿Qué significa?



## Entregables

- Herramientas
- Datos
- Informes

## Niveles

- Operacional
- Táctico
- Estratégico

## Reducir la superficie de ataque

identificando y corrigiendo vulnerabilidades externas

## Responder más rápidamente

Obtener contexto adicional sobre las alertas de seguridad, lo que mejora la respuesta a incidentes y reduce el MTTR (Tiempo Medio de Respuesta).

## Conocer lo desconocido

Identificar ataques fuera del alcance de los equipos internos de seguridad.

## Estar preparado para el futuro

Comprender la evolución de las tendencias de seguridad para implementar medidas de defensa proactivas.

## Conocer a tu adversario

Identifica quién puede atacarte según tu sector y ubicación. Comprende sus tácticas y técnicas para anticiparte y fortalecer tus defensas..

## Resiliencia cibernética

Mejorar la capacidad de resistir un ciberataque. Avanzar hacia la ciberinmunidad, donde el coste de atacar sea demasiado alto para los adversarios..

## Reducir el riesgo

Proporcionar a los principales responsables (CEO, CTO, CISO, CIO, Consejo de Administración) información esencial para orientar la inversión en ciberseguridad.

# Integraciones de fuentes de datos de seguridad de redes de Kaspersky



## Refuerce las soluciones de defensa de su red

con IoCs continuamente actualizados para bloquear automáticamente las ciberamenazas más prevalentes. Los Data Feeds se agregan a partir de fuentes consolidadas, heterogéneas y altamente fiables, como Kaspersky Security Network, nuestros web crawlers proactivos, el servicio de Monitorización de Botnets (monitorización 24/7/365 de botnets, objetivos y actividades asociadas), y los servicios de inteligencia sobre hosts e IPs.

## Evite la exfiltración de activos sensibles

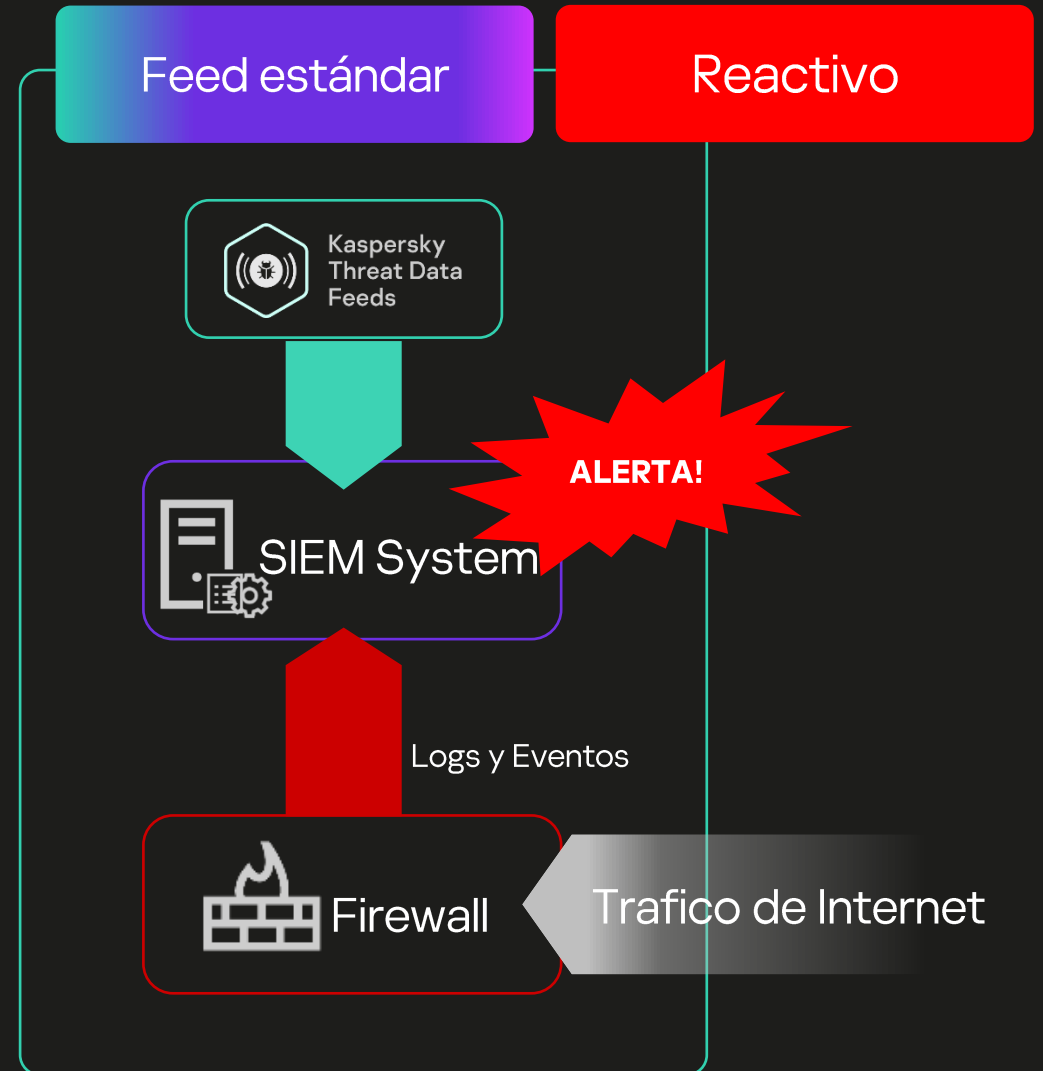
e información confidencial desde máquinas infectadas hacia fuera de su organización. Kaspersky ofrece colecciones especialmente diseñadas de IoCs que, al ser importadas en un NGFW, mejoran significativamente el nivel de protección de la red corporativa frente a amenazas comunes, sin necesidad de integraciones ni configuraciones complejas, y manteniendo la topología de red existente.

## Bloquee rápidamente las ciberameazas para proteger

su organización y garantizar la continuidad del negocio. Los Network Security Threat Data Feeds se basan en los [Kaspersky Threat Intelligence Data Feeds](#) y contienen listas actualizadas regularmente con distintos tipos de IoCs (direcciones IP y dominios). El uso de esta información permite monitorizar y bloquear el acceso de los usuarios a recursos de red peligrosos..

# Kaspersky Network Security Data Feeds – Feed Estándar

```
{
  "id": "Unique record identifier. (example: 143348)"
  "type": "Record type (matching rules are different for different types). (example: 1)"
  "mask": "Record covering malicious websites or web pages. (example: maliciousurl.com)"
  "category": "Category of the record. (example: Malware)"
  "first_seen": "Date when a record was created / detected (UTC). (example: 08.04.2014 16:45)"
  "last_seen": "Date when a record was last encountered by Kaspersky users (UTC). (example: 12.02.2015 13:56)"
  "popularity": "Record's popularity (how many users have been affected by a record). 5 is the most popular, 1 is the least popular. (example: 4)"
  "geo": "Top 10 countries where Kaspersky users were most affected by a record. (example: EN,FR,RU,GE,CH)"
  "IP": "Top 10 resolved IP addresses of a URL / mask within the last three months. (example: 192.168.0.1)"
  "files": "[Information about malicious files that were downloaded from the URL.
  {
    "MD5": "MD5 hash of a malicious file that was downloaded from the URL. (example: 2077AA102083676...36DC207C941)"
    "SHA1": "SHA-1 hash of a malicious file that was downloaded from the URL. (example: D08C43B778561AC8D91FF1AA...7C1A1)"
    "SHA256": "SHA256 hash of a malicious file that was downloaded from the URL. (example: 92D6457483E85D1E38272E91...20A17)"
    "threat": "Name of the detected object. (example: HEUR:Trojan.Script.Generic)"
  }
]
  "whois": {Domain's WHOIS and DNS data.
  "domain": "Domain name. (example: 12345.com)"
  "created": "Domain creation date. (example: 06.10.2013)"
  "updated": "Date when the WHOIS information for the domain was last updated or otherwise changed. (example: 11.10.2014)"
  "expires": "Expiration date. (example: 06.10.2015)"
  "name": "Person that registered the domain name (registrant). (example: Cheng Li)"
  "org": "Company that registered the domain name (registrant). (example: Cheng Li organization)"
  "country": "Registrant's country. (example: CHINA)"
  "city": "Registrant's city. (example: guangzhoushi)"
  "email": "Registrant's email address. (example: Posr1982@153.com)"
  "registrar_name": "Registrar's name. (example: GODADDY.COM, LLC)"
  "registrar_email": "Registrar's email address. (example: email@godaddy.com)"
  "NS": "Name server, which is an Internet record that is associated with a specific IP address. Name servers tell the public Internet where to find the used DNS record. (example: ns01.domaincontrol.com)"
  "NS_ips": "IP addresses of a name server. (example: 216.59.175.1, 208.159.245.9)"
  "MX": "Mail exchanger records (MX records). (example: mx1.domaincontrol.com)"
  "MX_ips": "IP addresses of a mail exchanger. (example: 217.69.175.2)"
  }
  "industry": "Top 10 industries targeted by the attack (example: Technology, Telecommunications, Energy)"
```



# Kaspersky Network Security Data Feeds – Feeds de Rede

IP:

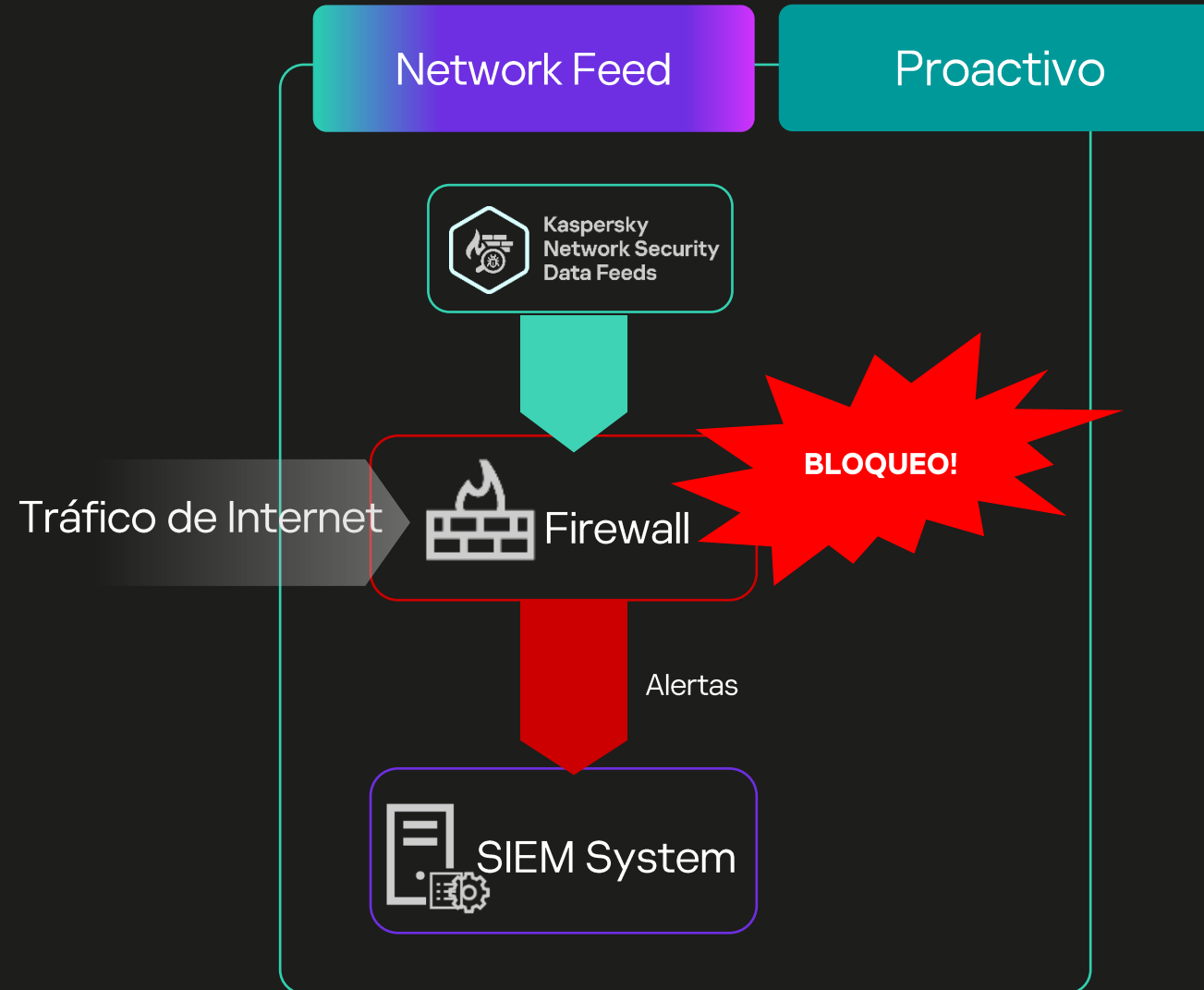
- 194.180.49.44
- 213.109.202.210
- 141.98.11.100
- 194.180.48.19
- 45.137.22.227
- 194.180.48.59

URL:

- saaadnesss.shop
- adult-empire.com
- dasyuredenmark.com
- dadarmy.sbs
- ceigix.com
- bunnycdn.b-cdn.net
- ak.ceegriwuwoa.net

PHISHING DOMAINS:

- zlibrary.to
- z-lib.io
- pringed.space
- regulationprivilegescan.top
- lectulandia.com
- superiorflirt.club
- webdaily.live
- r7862nks67.xyz
- xenoexecutor.com
- hot-survey.com
- lndk-a4.online



Reforzar las soluciones de defensa de la red





Se realizó una prueba con las reglas de detección integradas en FortiGate frente a 1000 reglas del Feed de Seguridad de Amenazas de Kaspersky Network Security.

The screenshot shows the Fortinet FortiView interface. On the left is a navigation menu with categories like Dashboard, Network, Policy & Objects, Addresses, and Security Profiles. The main area displays 'FortiView Policies by Bytes' for a specific policy named 'Lista Negra Bloqueados (43)'. It shows details like Policy Type (Firewall), Source Interface (lan), and Destination Interface (MOVISTAR (wan1)). Below this, there are tabs for Sources, Destinations, Applications, and Threats. The 'Destinations' tab is active, showing a table of IP addresses and their validity.

IP Address	Threat Feed Kaspersky	Entry	Validity
80.66.79.247			Valid
213.109.202.154			Valid
79.124.58.218			Valid
185.222.57.147			Valid
104.21.90.125			Valid
45.137.22.229			Valid
45.125.66.19			Valid
141.98.11.96			Valid
customer-rental.rootlayer.net (45.137.22.254)			Valid
185.222.58.238			Valid
62.204.41.230			Valid
45.143.223.133			Valid
91.92.247.130			Valid
185.222.57.90			Valid
141.98.10.127			Valid
eskerazyredp.online (93.185.167.134)			Valid
141.98.10.87			Valid
195.19.93.142			Valid
45.137.22.182			Valid
92.63.197.59			Valid
141.98.10.86			Valid
ip189.ip-176-31-46.eu (176.31.46.189)			Valid
79.137.202.179			Valid
176.97.210.185			Valid
185.222.57.75			Valid
91.92.250.14			Valid
45.137.22.113			Valid
95.214.26.35			Valid
185.155.184.208			Valid
163.123.143.87			Valid
172.67.156.164			Valid

## Resultados

Tasa de detección exitosa por

# 47.7%

El Feed de Seguridad de Amenazas de Kaspersky Network Security proporciona un aumento adicional en la tasa de detección de:

# 52.3%



Se realizó una prueba en un Palo Alto PA-220 con 1000 reglas del Feed de Seguridad de Amenazas de Kaspersky Network Security, con las siguientes listas de detección de Palo Alto activadas:

The screenshot shows the Palo Alto Networks PA-220 management interface. A modal window titled "Listas de bloqueo dinámicas" (Dynamic Blocking Lists) is open, displaying the configuration for a list named "Kaspersky\_tip\_IP". The "List Entries And Exceptions" tab is active, showing a search bar with "19235 eleme" and a list of IP addresses under "ENTRADAS DE LISTA". The list includes:

- 185.222.58.44
- 45.137.22.254
- 193.200.78.24
- 185.222.58.237
- 137.74.52.226
- 185.29.10.26
- 170.79.181.188

At the bottom of the modal, there are buttons for "Probar URL de origen", "ACEPTAR", and "Cancelar". The background interface shows a table of dynamic lists with columns for "NOMBRE", "UBICACIÓN", "DESCRIPCIÓN", "IP ORIGEN", "PERFIL DEL CERTIFICADO", and "FRECUENCIA".

## Resultados

Tasa de detección exitosa por

# 51.3%

El Feed de Seguridad de Amenazas de Kaspersky Network Security proporcionó un aumento adicional en la tasa de detección de:

# 47.9%

# Kaspersky Network Security Data Feeds – ¿Para quién fue desarrollado?



## MSP/MSSP

Empresas que ofrecen servicios de seguridad gestionada, incluyendo la administración de endpoints, firewalls, correo electrónico y formación en concienciación sobre seguridad.

## Beneficio

Los MSP/MSSP que operan un firewall gestionado obtienen una mayor tasa de detección en el perímetro, ayudando a prevenir infecciones y a reducir el MTTD (Tiempo Medio de Detección).



## Pequeñas/Medias Empresa

Organizaciones con un equipo de TI pequeño o mediano, pero sin un SOC (Centro de Operaciones de Seguridad). Disponen de presupuestos ajustados para soluciones de ciberseguridad.

## Beneficio

Las organizaciones SMB/Small/Ent pueden mejorar significativamente sus tasas de detección en red sin necesidad de realizar una gran inversión. La integración sencilla y la gestión simplificada reducen el coste total de propiedad (TCO).



## Grandes Empresas

Organizaciones con capacidades de SOC y monitorización de seguridad ya establecidas.

## Beneficio

Las grandes empresas pueden mejorar el bloqueo de amenazas en el perímetro, lo que reduce el MTTD y disminuye la carga de investigaciones internas.

Industrias

TODAS

# ¡Muchas Gracias!



**Kaspersky  
Network Security  
Data Feeds**



Pedro Jorge Viana de Bragança  
Head of Presales  
Spain and Portugal