José Carlos López Henestrosa

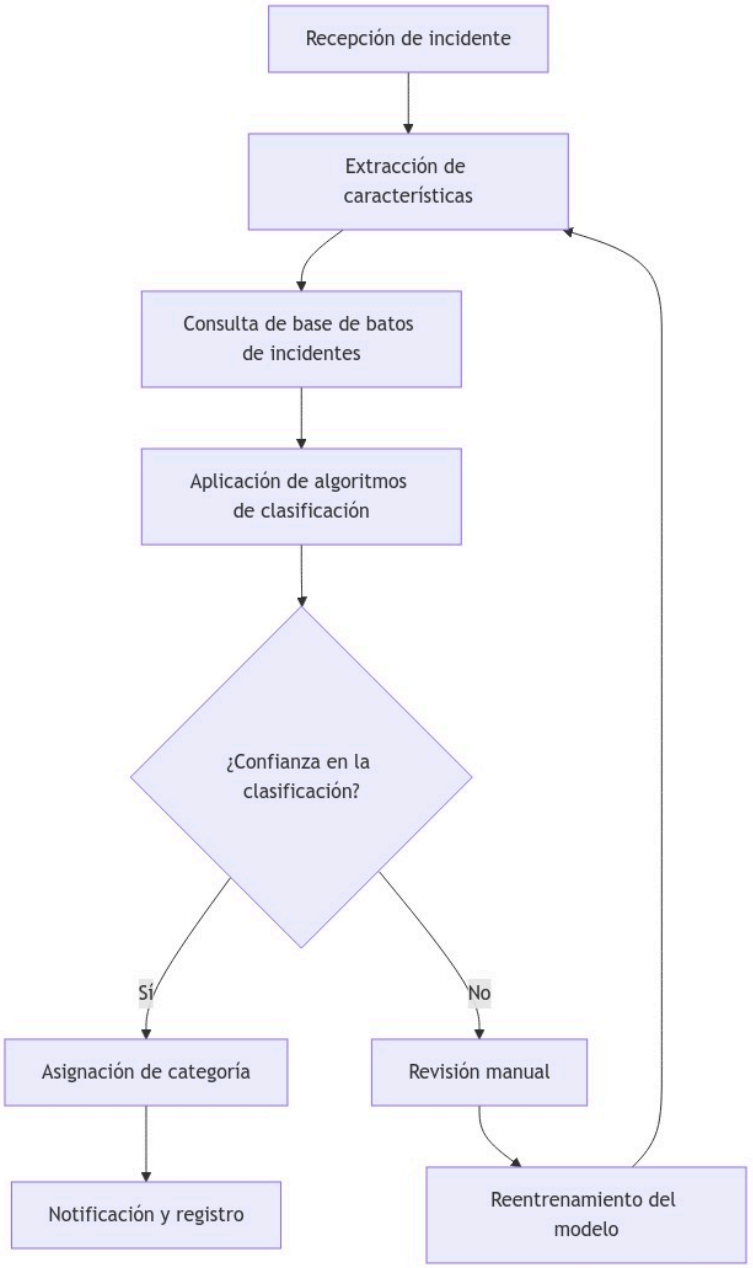
Incidentes de ciberseguridad

Tarea 2: Auditoría de incidentes de ciberseguridad

Índice

Diseño del Diagrama de Bloques del Clasificador Automático de Incidencias

Diseña el Diagrama de Bloques del sistema a alto nivel. El objetivo de esta tarea es proporcionar la información básica de análisis para que los Técnicos Informáticos puedan desarrollar el sistema clasificador.



Describe a alto nivel la funcionalidad en general y de cada bloque propuesto (sin entrar en detalle).

El bloque central del diagrama de flujo muestra el ciclo que va desde la obtención de los requisitos a través de la extracción de características del incidente hasta la aplicación de la inteligencia mediante algoritmos de clasificación. Dentro de este proceso, hemos desglosado cada paso en el Diagrama de Bloques propuesto más arriba, en el que distinguimos los siguientes puntos:

1. **Recepción de incidente**: Recibe incidentes reportados desde diversas fuentes.
2. **Extracción de características**: Extrae información clave del incidente para su análisis.
3. **Consulta de base de datos de incidentes**: Consulta incidentes previos para contextualizar el caso.
4. **Aplicación de algoritmos de clasificación:** Aplica algoritmos de clasificación para determinar la categoría del incidente.
5. **¿Confianza en la clasificación?**: Evalúa si la clasificación alcanzó un nivel aceptable de confianza.
6. **Asignación de categoría**: Asigna la categoría correspondiente si la clasificación es confiable.
7. **Revisión manual**: En caso de baja confianza, se envía a revisión manual.
8. **Reentrenamiento del modelo:** Los incidentes revisados manualmente pueden ser usados para mejorar el modelo.
9. **Notificación y registro:** Finalmente, el incidente se notifica y registra en el sistema.

Diseño del interior del bloque central con herramientas OSINT

Teniendo en cuenta que el Clasificador Automático pertenece a una empresa ficticia (invéntate el nombre y dominio en internet) y que incorpora un bloque central, deberás efectuar las siguientes tareas:

Describe detalladamente las funciones a realizar por el bloque central dentro del Diagrama de Bloques propuesto en el apartado anterior.

Ahora que sabemos la funcionalidad en general a alto nivel del bloque central, nos adentramos en cada función en más detalle:

1. **Recepción de incidente**: Este es el primer paso del proceso. Se encarga de captar y registrar los incidentes que llegan al sistema. La recepción puede realizarse de varias formas, las cuales dependen de la fuente del incidente. Dentro de las fuentes, podemos distinguir, principalmente, los reportes manuales y los sistemas de monitoreo automático.

   Durante esta etapa, es importante detallar la descripción del incidente y recopilar datos clave, como el usuario afectado, el nivel de urgencia o la fecha y hora del incidente. Una vez se verifica que esta información es completa y comprensible, se envía a la siguiente fase para su análisis automático.

2. **Extracción de características**: Este paso se encarga de analizar el incidente recibido y extraer datos relevantes que puedan ayudar en su clasificación. Se puede llevar a cabo gracias a los logs y registros del sistema, a partir de los cuales se puede aplicar análisis de texto para extraer palabras clave que puedan ayudar a identificar el tipo de incidente.

3. **Consulta de base de datos de incidentes**: Aquí se accede a una base de datos histórica que almacena información sobre incidentes previos para buscar patrones similares y ayudar en la clasificación. Si el incidente tiene características similares a eventos pasados, se puede recuperar la categoría y la solución asociada.

4. **Aplicación de algoritmos de clasificación**: Este procedimiento emplea modelos de aprendizaje automático o reglas definidas para asignar una categoría inicial al incidente. Dichos modelos devuelven una clasificación junto con una medida de certeza o confianza en la predicción, por lo que durante el post-procesamiento de resultados se puede hacer una combinación de predicciones para mejorar la precisión.

5. **¿Confianza en la clasificación?**: Dependiendo del resultado de dicha clasificación, podemos asignar la categoría automáticamente, en caso de que la confianza sea alta. Por otro lado, si la confianza es baja, el incidente pasaría a revisión manual, que posteriormente serviría para reentrenar el modelo y mejorar la precisión futura.
6. **Asignación de categoría**: Ocurre cuando la confianza en la clasificación automática es lo suficientemente alta, tal y como hemos puntualizado anteriormente. Aquí, el sistema asigna una categoría predefinida específica al incidente. Dependiendo de la categoría, se puede atribuir un nivel de urgencia determinado para su resolución y asignárselo a una persona o equipo concreto para su gestión.
7. **Notificación y registro**: Una vez que el incidente ha sido categorizado correctamente, se notifica a las partes interesadas y se registra en la base de datos. Dependiendo de la criticidad del incidente, se pueden activar procesos de escalamiento y generar reportes sobre la cantidad y tipo de incidentes recibidos.
8. **Revisión manual**: Si la confianza en la clasificación es baja, el incidente se envía a un analista humano para su revisión y categorización manual. Asimismo, el analista puede añadir más detalles que no fueron detectados automáticamente, como notas o contexto adicional del incidente, las cuales son almacenadas para mejorar el modelo en futuras clasificaciones.
9. **Reentrenamiento del modelo**: Durante este proceso, se busca mejorar la precisión del modelo utilizando nuevos datos obtenidos de la revisión manual y los incidentes clasificados correctamente. Para ello, se optimizan los parámetros del modelo para mejorar su precisión y se vuelve a entrenar con los datos actualizados. Posteriormente, se mide la precisión y la capacidad del modelo optimizado para clasificar correctamente incidentes nuevos.

Propón las acciones de búsqueda que debe realizar el bloque central para realizar búsquedas automáticas en Google de la siguiente información:

Archivos Excel con macros (`.xlsm`) que se alojen en páginas no seguras.

Con el fin de realizar las búsquedas automáticas en Google, el bloque central debe emplear Google Dorking, lo cual es una técnica que consiste en aplicar la búsqueda avanzada de Google para conseguir encontrar en Internet información concreta a base de ir filtrando los resultados con operadores conocidos como *Dorks*, que son símbolos que especifican una condición. Por ejemplo, si ponemos en nuestro texto de búsqueda las dobles comillas (“texto”), buscará información que coincida exactamente con el texto. Es decir, si buscamos “OSI”, nos devolverá el contenido que concuerde exactamente con ese término. También podemos acceder a la búsqueda avanzada a través de este enlace.

Dicho esto, pasamos a plantear la búsqueda adecuada para el caso propuesto.

Para encontrar este formato de archivos alojados en sitios web no seguros (HTTP en lugar de HTTPS), podemos utilizar la siguiente búsqueda:

```
filetype:xlsm "macro" inurl:http
```

Donde:

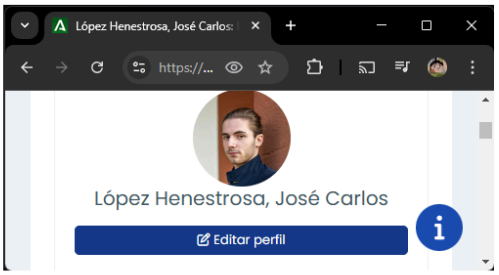
- `filetyppe:xlsm` → Busca exclusivamente archivos con extensión `.xlsm`.
- `"macro"` → Busca páginas donde aparezca la palabra "macro" en el contenido. Esto aumenta las probabilidades de encontrar archivos que contienen macros.
- `inurl:http` → Asegura que la URL contenga estrictamente el protocolo HTTP (páginas no seguras)

Google filetype:xlsm "macro" inurl:http

Iniciar s

Todo Imágenes Vídeos Noticias Libros Web Finanzas Herramientas

Sugerencia: Mostrar resultados en **español**. También puedes consultar más información sobre cómo filtrar por idioma.



Texas Tech University
http://rritchey.ba.ttu.edu › FIN5320 › FinMath XLS

Macro

Always SAVE workbook as .xlsm before recording a **macro!** 3, PRACTICE the keystrokes before recording. 4, When ON the Use Relative References Button allows ...

illesbalears.cat
http://www.illesbalears.cat › finestretarenovables XLS

Indicaciones de cumplimentación

La configuración de la **macro** no cambia para todos los programas de Office. 17. 18, 1. Haga clic en la pestaña Archivo. 19, 2. Haga clic en Opciones .

hosting.co.za
http://deptfinweb01.onsite.hosting.co.za › MACROS XLS

Macro to insert missing formulas on personnel sheet and ...

This should be implemented by all departments. The **macro** will effect the following adjustments to the workbook: - On all programme sheets, correct the formula ...

SAS Institute
http://ftp.sas.com › drugdev › lsafmacroapi24 › L... XLS

LSAF Macros 2.4 Changes

Macro name, input parameters, and/or returned results changed. 297, Deprecated, **Macro** functionality has been replaced by another **macro**. **Macro** is flagged to be ...

International Journal of Design
http://www.ijdesign.org › materials › 4171_Appe... XLS

T1 Analysis

... sectoral or organizational level), state, low, medium, high. 7, **Macro** (e.g. field or national level), profession, low, medium, high. 8, community, low, medium ...

Sistema de Información de Precios al Consumidor
http://www.precios.uy › cadenas_agosto_2021 XLS

Hoja1

Macro, Micro **Macro**, Pigalle, San Roque, Ta - Ta, Tienda Inglesa. 3, Aceite de girasol Óptimo Envase 900 cc, 118, 122, 118, 112, 112, --, --, --, 119, 112.87 ...

| Konsortium der Schweizer Hochschulbibliotheken
http://consortium.ch › acs_titlelist_publish XLS

Title list

ACS **Macro** Letters, 2161-1653, https://pubs.acs.org/journal/amlccd. 39, ACS Materials Au1, 2694-2461, https://pubs.acs.org/acsmaterialsau. 40, ACS Materials ...

hosting.co.za
http://deptfinweb01.onsite.hosting.co.za › templates XLS

Macro to insert missing formulas on personnel sheet and ...

Run **Macro!** ... **Macro** ...

EPMHV
http://www.epmhv.gob.ec › web › content XLS

listas

27 ago 2024 — Nombre Proyecto/ **Macro** actividad, Código Nombre Proyecto/ **Macro** actividad, Código Nombre Componente /Actividad, Código Nombre Componente ...

Lixoft
http://lixoft.com › filesToWebsite › documentation XLS

AdaptData

The **macro** checks that time intervals are continuous (no gaps allowed). Only the column END TIME should be used as TIME in PKanalix. * In case of censored ...

Goooooooooogle ›
1 2 3 4 5 6 7 8 9 10 Siguiente

Busca en https://pastebin.com correos electrónicos pertenecientes al nombre de tu empresa y excluye las direcciones de Gmail y Hotmail.

Dado que Google indexa el contenido de Pastebin, se puede utilizar la siguiente consulta para buscar direcciones de correo electrónico con el dominio de nuestra empresa (supongamos que el nombre de la empresa es Tesla, cuyo dominio de correo es `@tesla.com`) y excluir direcciones de Gmail y Hotmail:

```
site:pastebin.com "@tesla.com" -"@gmail.com" -"@hotmail.com"
```

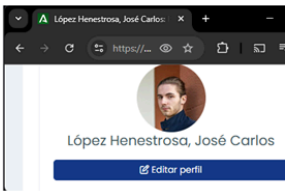
Donde:

- `site:pastebin.com` → Limita la búsqueda a Pastebin.
- `"@tesla.com"` → Busca correos que contengan el nombre de la empresa. En este caso, voy a utilizar una con renombre, como Tesla, para obtener más resultados en la búsqueda.
- `-"@gmail.com" -"@hotmail.com"` → Excluye correos de Gmail y Hotmail.

Google

site:pastebin.com "@tesla.com" -"@gmail.com" -"@hotmail.com"

Todo Imágenes Vídeos Noticias Web Libros Finanzas Herramientas



Pastebin
https://pastebin.com › ... · Traducir esta página

Tesla Sources - Pastebin.com

1 nov 2021 — https://www.**tesla.com**/cybertruck/design#battery. https://ir.**tesla.com**/press-release/tesla-motors-launches-revolutionary-supercharger-enabling.

Pastebin
https://pastebin.com › ... · Traducir esta página

Tesla apk - Pastebin.com

Для получения дополнительной информации о Tesla, посетите www.**tesla.com**. Безопасность данных. Чтобы контролировать безопасность, нужно знать, как разработчики ...

Pastebin
https://pastebin.com › ... · Traducir esta página

api-toolbox.tesla.comappplayer.tesla.comautobidder-eng. ...

18 mar 2020 — ciscoguest.**tesla.com**. click.emails.**tesla.com**. dev.**tesla.com**. employeefeedback.**tesla.com**. energysupport.**tesla.com**. eua-origin.**tesla.com**. eumirror ...

Pastebin
https://pastebin.com › ... · Traducir esta página

Tesla Video/Report Sources - Pastebin.com

14 nov 2022 — Tesla Video/Report Sources · https://www.youtube.com/watch?v=RTZdzFCmlgs · https://www.**tesla.com** · https://www.**tesla.com**/blog/introducing-megapack- ...

Pastebin
https://pastebin.com › ... · Traducir esta página

tm=2019-10-13 11:00:40348 ip=192.168.90.125 user= ...

18 oct 2019 — ... **tesla.com**']), ('help', 'toolbox**@tesla.com**'), ('error_from', 'toolbox-errors**@tesla.com**')], 'logging': [('toolbox', {'level': 'INFO'}), ('root ...

Pastebin
https://pastebin.com › ... · Traducir esta página

20.8 release notes - Pastebin.com

Send email to navfeedback**@tesla.com**, or press the voice commands button on the right side of the steering wheel and say "Note," followed by your comments.

Pastebin
https://pastebin.com › ... · Traducir esta página

<?php$to = "кому";$subject = "Заголовок";$message ...

1 oct 2018 — $message = "Текст сообщения";. $headers = "From: Elon Musk <admin**@tesla.com**>\r\nContent-type: text/plain; charset ...

Pastebin
https://pastebin.com › ... · Traducir esta página

How Tesla Semi Will Devastate Long Haul Trucking

https://www.**tesla.com**/semi. https://www.chooseenergy.com/electricity-rates-by-state/. https://www.trucks.com/2016/11/29/electronic-logging-devices-truckers ...

Pastebin
https://pastebin.com › ... · Traducir esta página

describe("routes : posts", () => { beforeEach((done) => { this ...

13 may 2019 — then((res) => {. User.create({. email: "starman**@tesla.com**",. password: "Trekkie4lyfe". }) .then((user) => {. this.user = user;. Topic.create ...

Pastebin
https://pastebin.com › wjakJwg5 · Traducir esta página

Elon Musk GFS Sources - Pastebin.com

14 mar 2017 — https://www.**tesla.com**/de_DE/about. https://www.**tesla.com**/de_DE/. https://en.wikipedia.org/wiki/Tesla_Autopilot. https://www.**tesla.com**/de_DE/ ...

En respuesta a las diversas reclamaciones recibidas en relación con la ley estadounidense de protección de los derechos de autor (DMCA), hemos retirado 4 resultados de esta página. Si quieres, puedes leer las reclamaciones de la DMCA que han originado la retirada de estas páginas en LumenDatabase.org: Reclamación, Reclamación, Reclamación, Reclamación.

Ficheros SQL con volcado de una base de datos, excluyendo GitHub.

Para ello, podemos usar:

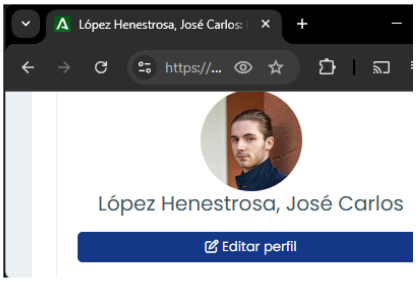
```
filetype:sql "-- phpMyAdmin SQL Dump" | "create table" -site:github.com
```

Donde:

- `filetype:sql` → Busca archivos con extensión `.sql`.
- `"-- phpMyAdmin SQL Dump"` → Filtra resultados que contienen la firma de un volcado generado por phpMyAdmin.
- `"create table"` → Filtra volcados que contienen estructuras de base de datos.
- `-site:github.com` → Excluye resultados provenientes de GitHub.

Google filetype:sql "-- phpMyAdmin SQL Dump" | "create table" -site:github.com

Todo Imágenes Vídeos Noticias Web Libros Finanzas



Universidad de Sevilla
https://biblus.us.es › proyectos › abreproy › fichero

bbddJARA_MyISAM.sql

... **CREATE TABLE** `acciones` (`id_accion` int(10) NOT NULL auto_increment, `nombre` varchar(20) collate latin1_general_ci NOT NULL default '', `descripcion` ...

Lebanese University
http://droit2.ul.edu.lb › phpmyad... · Traducir esta página

phpMyAdmin SQL

-- **phpMyAdmin SQL Dump** -- version 3.3.2deb1ubuntu1 -- http://www.phpmyadmin ... **CREATE TABLE** IF NOT EXISTS `pma_bookmark` (`id` int(11) NOT NULL ...

Universidad de Sevilla
https://biblus.us.es › proyectos › use › abreproy › fichero

carpooldb.sql

-- **phpMyAdmin SQL Dump** -- version 3.4.5 -- http://www.phpmyadmin.net ... **CREATE TABLE** IF NOT EXISTS `carpool` (`ref_number` varchar(8) NOT NULL ...

สำนักงาน กศน. จังหวัดเพชรบูรณ์
http://phetchabun.nfe.go.th › scripts · Traducir esta página

create_tables.sql

... **CREATE TABLE** `pma_bookmark` (`id` int(11) NOT NULL auto_increment, `dbase` varchar(255) NOT NULL default '', `user` varchar(255) NOT NULL default ...

Opticon USA
http://ftp.opticonusa.com › esl · Traducir esta página

mysql_sample_table_products.sql

-- **phpMyAdmin SQL Dump** -- version 4.2.7.1 -- http://www.phpmyadmin.net ... **CREATE TABLE** IF NOT EXISTS `products` (`NotUsed` varchar(1), `ProductId` ...

Universidad Técnica Federico Santa María
http://profesores.elo.utfsm.cl › QuirozFerrada › descargas

tablas.sql

28 nov 2009 — -- **phpMyAdmin SQL Dump** -- version 3.2.0.1 -- http://www.phpmyadmin ... **CREATE TABLE** IF NOT EXISTS `Alumnos` (`Rut` int(11) NOT NULL ...

Comisión Bicameral de Presupuesto
https://bicameral.congreso.gov.py › ... · Traducir esta página

mysql.sql

-- **phpMyAdmin SQL Dump** -- version 2.11.6 -- http://www.phpmyadmin.net ... **CREATE TABLE** IF NOT EXISTS `message` (`message_id` bigint(20) unsigned NOT ...

International Centre for Numerical Methods in Engineering (CIMNE)
http://www2.cimne.com › security · Traducir esta página

http://www2.cimne.com/chameleon/common/security/se...

... **CREATE TABLE** com_profile (id int(11) NOT NULL auto_increment, user_name varchar(50) NOT NULL default '', password varchar(25) NOT NULL default '', address1 ...

UOC
https://openaccess.uoc.edu › GID · Traducir esta página

https://openaccess.uoc.edu/bitstream/10609/6541/4/...

... **create table** t_adsl (dsl_id smallint not null auto_increment, tel_id smallint, dsl_vel numeric(4,2), primary key (dsl_id), unique key uk_dsl_tel (tel_id) ...

gob.mx
http://www.conabio.gob.mx › snib › modelo › CONABI...

Creación del modelo, script para MySQL

... **CREATE TABLE** CatalogoEjemplar (IdCatEjemplar int NOT NULL , Descripcion VARCHAR(255) NOT NULL , Nivel1 int NOT NULL , Nivel2 int NOT NULL , Nivel3 int NOT ...

Goooooooooogle ›
1 2 3 4 5 6 7 8 9 10 Siguiente

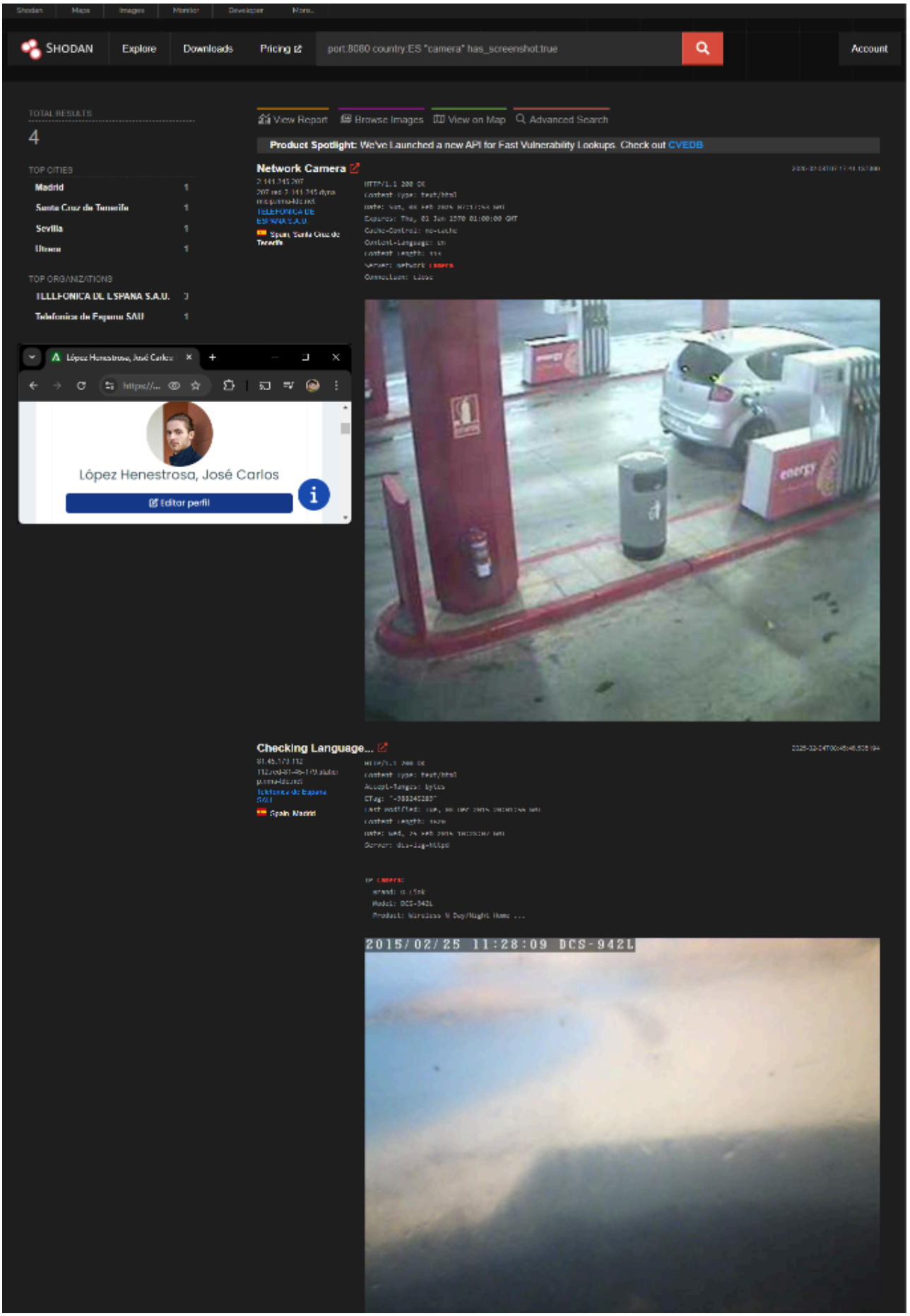
Propón que el sistema compruebe los dispositivos conectados a Internet que tengan el puerto 8080 abierto, dispongan de una captura de imagen y estén ubicados en España.

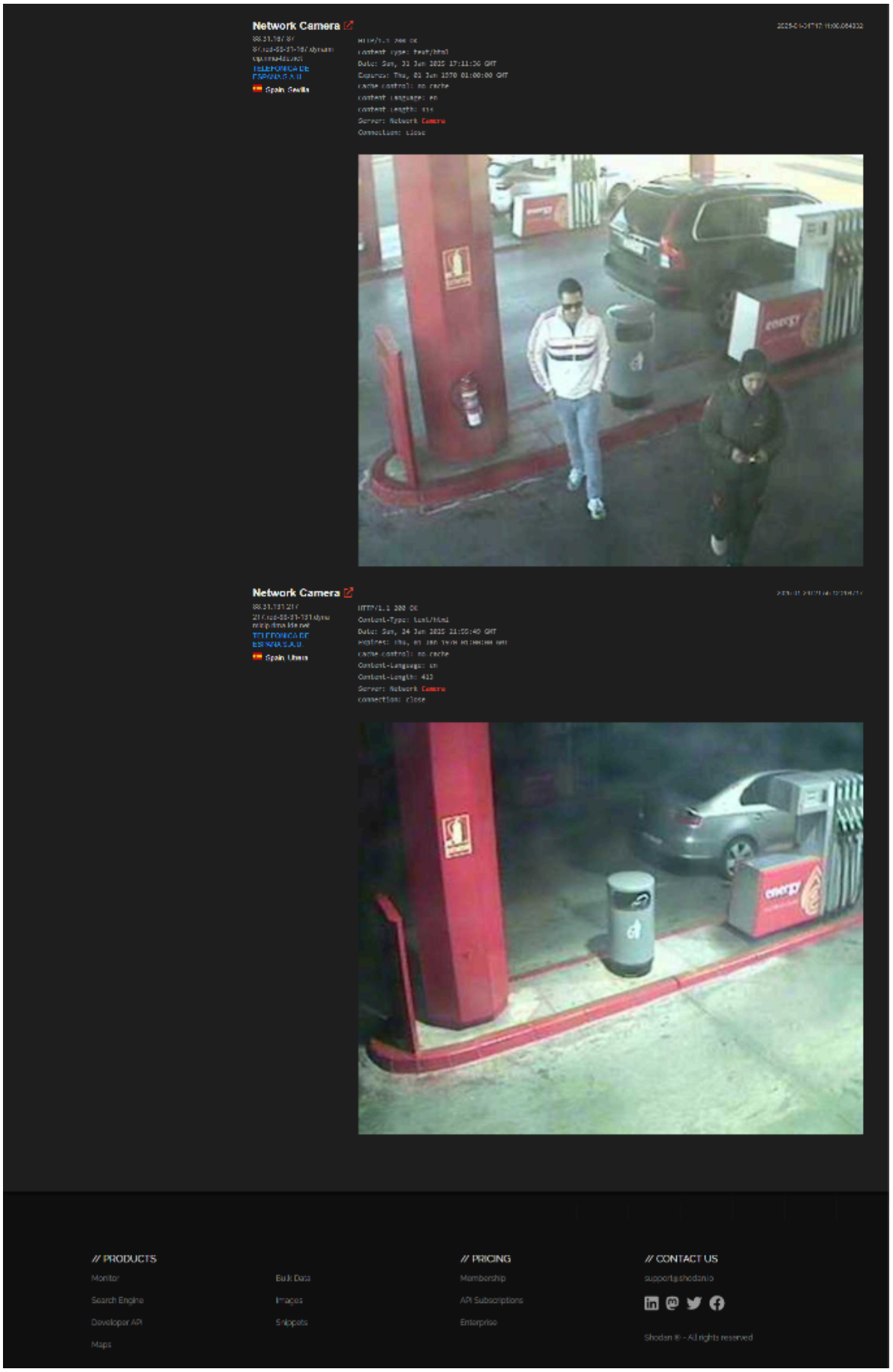
Para conseguir esto, podemos usar Shodan, el cual es un motor de búsqueda que indexa dispositivos conectados a Internet. Para realizar la consulta planteada en el enunciado, podemos hacer lo siguiente:

```
port:8080 country:ES "camera" has_screenshot:true
```

Donde:

- `port:8080` → Filtra dispositivos que tienen el puerto 8080 abierto.
- `country:ES` → Limita los resultados a España.
- `"camera"` → Busca específicamente cámaras.
- `has_screenshot:true` → Busca cámaras que tienen una captura de pantalla asociada en la base de datos de Shodan.


SHODAN
Explore
Downloads
Pricing
port:8080 country:ES "camera" has_screenshot:true
Account
TOTAL RESULTS
4
TOP CITIES
Madrid 1
Santa Cruz de Tenerife 1
Sevilla 1
Ulldecona 1
TOP ORGANIZATIONS
TELEFONICA DE ESPANA S.A.U. 3
Telefonica de Espana SAU 1
View Report
Browse Images
View on Map
Advanced Search
Product Spotlight: We've Launched a new API for Fast Vulnerability Lookups. Check out CVEDB
Network Camera
López Henestrosa, José Carlos
Editar perfil
Checking Language...
Spain, Madrid
2015/02/25 11:28:09 DCS-942L


Network Camera
Spain Seville
Content-Type: text/html
Server: Network Camera
Connection: close
Network Camera
Spain Ubeda
HTTP/1.1 200 OK
Content-Type: text/html
Content-Language: en
Content-Length: 413
Server: Network Camera
connection: close
// PRODUCTS
Monitor
Search Engine
Developer API
Maps
Bulk Data
Images
Snippets
// PRICING
Membership
API Subscriptions
Enterprise
// CONTACT US
support@shodan.io
Shodan ® - All rights reserved

Bibliografía

- INCIBE. (2014, 28 de mayo). *OSINT - La información es poder*. https://www.incibe.es/incibe-cert/blog/osint-la-informacion-es-poder
- INCIBE. (2023, 15 de marzo). *Google Dorks te ayuda a encontrar información sobre ti en la Red*. https://www.incibe.es/ciudadania/blog/google-dorks-te-ayuda-encontrar-informacion-sobre-ti-en-la-red
- AVG. (2022, 14 de octubre). *Google dorks: ¿Qué son los Google Hacks y cómo se utilizan?* https://www.avg.com/es/signal/google-dorks
- Autumn Skerritt. (2023, 11 de junio). *Shodan - The Complete Guide, Featured on TryHackMe.* https://skerritt.blog/shodan/