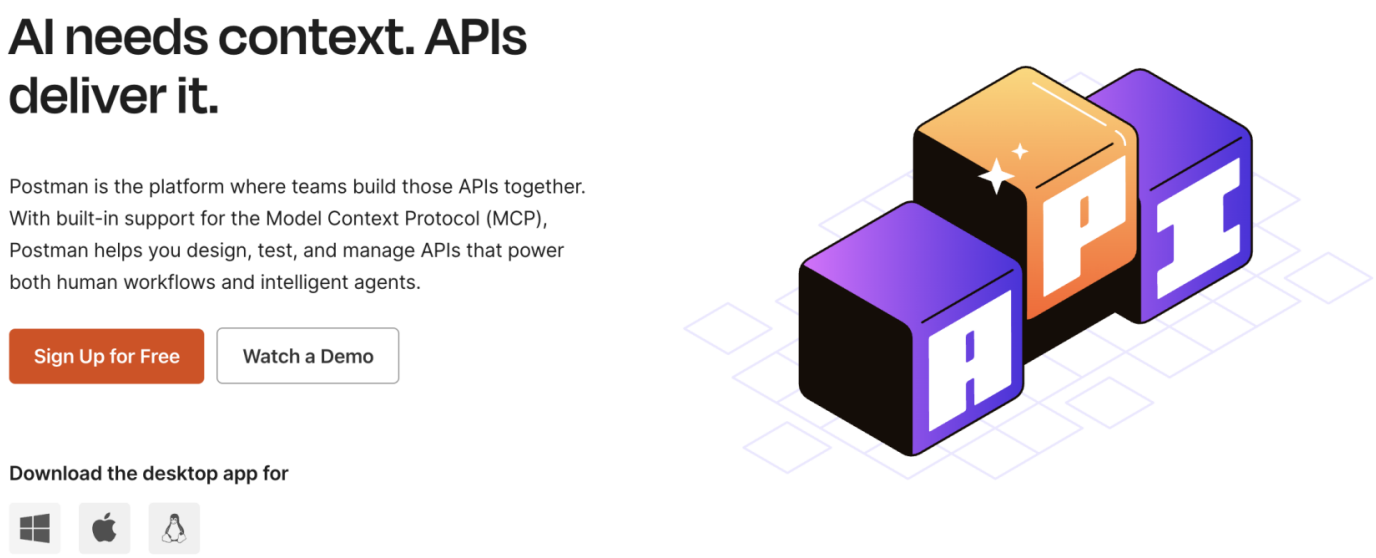
Triángulo del Fraude como servicio API

The Fraud Explorer posee una API capaz de prestar varios servicios, entre ellos el de la analítica del triángulo del fraude con FraudGPT.

Requisitos

Para trabajar con la API de The Fraud Explorer se requieren conocimientos en el consumo de APIs y un software que permita realizar consultas a APIs. En cuanto al software, se recomienda descargar **Postman**.



Respecto al conocimiento, se recomienda que las personas que harán uso delas API conozcan la arquitectura **REST**, que sepan cómo funciona el protocolo **HTTP** y el formato de texto **JSON**.

The Fraud Explorer es un software que junto con **FraudGPT** detecta el fraude y la corrupción en las organizaciones

Arquitectura

The Fraud Explorer está diseñado para permitir a sistemas de terceros consumir sus datos y realizar operaciones CRUD (**Create**, **Read**, **Update** y **Delete**) sobre sus registros tanto en la base de datos relacional como en la no estructurada.

A continuación en la tabla se resumen las capacidades de la arquitectura **REST** implementada en la solución:

Modulo	Operaciones disponibles
Endpoints	Leer datos de un Endpoint, leer todos los datos, crear un endpoint, eliminar un endpoint y actualizar el estado de un endpoint, teniendo en cuenta los permisos a través de la autenticación y su contexto.
Eventos y Alertas	Leer los eventos de un endpoint o de todos los endpoints presentados por el motor de Fraud Triangle Analytics. También se pueden leer las alertas generadas por el motor de inferencia del sistema de inteligencia artificial.
Workflows	Obtener el listado de los workflows existentes y obtener las alertas que han sido detectadas por los workflows. Los workflows son reglas que permiten crear una alerta si cumple con ciertas condiciones. Los workflows pueden correlacionar varias alertas y varias personas y es la forma más compleja y flexible de generación de alertas en The Fraud Explorer.
Triángulo del Fraude	Enviar datos de tipo semánticos para ser procesados en tiempo real y devolver los insights sobre el triángulo del fraude, incluyendo análisis de tono, relevancia, urgencia y probabilidad arrojada por la inteligencia artificial.
Model Context Protocol	Obtener un resumen general y detallado sobre las alertas de fraude y corrupción que ya han sido validadas no solo por FraudGPT sino por humanos. Estas alertas estarían listas para ser integradas en ciclos formales de User Behavior Analytcis que lleve la empresa sobre todos los activos de la organización.

Se recomienda el uso del software **Postman**, en el cual deberá preparar el ambiente (Collections) para poder ejecutar las operaciones. Actualmente los métodos soportados son **GET**, **PUT**, **POST** y **DELETE**.

The Fraud Explorer es un software que junto con **FraudGPT** detecta el fraude y la corrupción en las organizaciones

Servicios web

Listado de los webservice disponibles y cómo se usan

Gestión de endpoints

Antes de intentar consumir este servicio debe indicar en las cabeceras de la petición (**headers**) los parámetros de autenticación para identificarse ante el sistema. Use la llave **username** para indicar el nombre de usuario (con el mismo que inicia sesión en la interfaz web y **password** para indicar su contraseña.

Algunas consultas deben tener las siguientes cabeceras. Más abajo en la tabla de operaciones se indican cuales de ellas son necesarias dependiendo de la operación.

Header	Valor	Explicación
page	1	Consultar pagina numero 1
size	100	Ventana de resultados por pagina
datefrom	2022-01-01	Rango de fecha "desde"
dateto	2022-02-28	Rango de fecha "hasta"

Para que el intercambio de datos entre el cliente y el servidor sea legible, use adicionalmente la cabecera **Content-Type** con el valor **application/json**.

Operación	Método	Headers	URL Ejemplo
Obtener datos de un endpoint	**GET**	**username, password, page, size**	https://url/rest/endPoints?query=jason
Obtener los datos de todos los endpoints	**GET**	**username, password, page, size**	https://url/rest/endPoints?query=all
Crear o actualizar un endpoint	**PUT**	**username, password**	https://url/rest/endPoints?query=create&token=TOKEN&os=6.1&v=1.3.1 &domain=mydomain.loc&id=jason_abn76dk_agt&ip=172.16.1.1
Eliminar un endpoint	**DELETE**	**username, password**	https://url/rest/endPoints?query=delete&endpoint=jason

Este servicio web se usa para crear un agente personalizado, es decir, el cliente (organización) puede desarrollar clientes que envíen datos a The Fraud Explorer y para ello el primer paso es crear el agente, luego, se tienen disponibles otras operaciones administrativas para realizar eliminaciones de agentes, actualización de datos y obtención de información.

Este servicio web normalmente no será usado por las organizaciones y sí usado comunmente por nuestro equipo de NOFRAUD para el desarrollo de nuevos agentes para The Fraud Explorer.

The Fraud Explorer es un software que junto con **FraudGPT** detecta el fraude y la corrupción en las organizaciones.

Consulta de alertas

Antes de intentar consumir un servicio debe indicar en las cabeceras de la petición (**headers**) los parámetros de autenticación para identificarse ante el sistema. Use la llave **username** para indicar el nombre de usuario (con el mismo que inicia sesión en la interfaz web y **password** para indicar su contraseña.

Algunas consultas deben tener las siguientes cabeceras. Más abajo en la tabla de operaciones se indican cuales de ellas son necesarias dependiendo de la operación.

Header	Valor	Explicación
page	1	Consultar pagina numero 1
size	100	Ventana de resultados por pagina
datefrom	2022-01-01	Rango de fecha "desde"
dateto	2022-02-28	Rango de fecha "hasta"

Las operaciones disponibles son:

Operación	Método	Headers	URL Ejemplo
Obtener los eventos de un endpoint	**GET**	**username, password, page, size, datefrom, dateto**	https://url/rest/ftaEvents?endpoint=jason
Obtener los eventos de todos los endpoints	**GET**	**username, password, page, size, datefrom, dateto**	https://url/rest/ftaEvents?endpoint=all
Obtener las alertas de AI de un endpoint	**GET**	**username, password, page, size, datefrom, dateto**	https://url/rest/ftaEvents?ai=jason
Obtener las alertas de AI de los endpoints	**GET**	**username, password, page, size, datefrom, dateto**	https://url/rest/ftaEvents?ai=all

The Fraud Explorer es un software que junto con **FraudGPT** detecta el fraude y la corrupción en las organizaciones.

Envío de datos semánticos

Antes de intentar consumir este servicio debe indicar en las cabeceras de la petición (**headers**) los parámetros de autenticación para identificarse ante el sistema. Use la llave **username** para indicar el nombre de usuario (con el mismo que inicia sesión en la interfaz web y **password** para indicar su contraseña.

Para enviar datos semánticos de un endpoint para ser procesadas por The Fraud Explorer, debe usar la URL https://demo.thefraudexplorer.com/rest/endPoints?id=agent_ahsg17_agt con método **POST** y enviar en el **BODY** del mensaje lo siguiente:

```
{
 "hostPrivateIP":"10.20.23.8",
 "userDomain":"mydomain.loc",
 "appTitle":"Outlook",
 "phrases":"Aqui todos dicen que cerremos la boca pero yo te estoy contando, saludos"
}
```

Se supone que antes de enviar estos datos ya debió haber creado el endpoint previamente (lea la primera página de gestión de endpoints en este mismo capítulo).

El id del endpoint deberá ser exactamente igual al indicado al momento de la creación den endpoint.

Analítica del triángulo del fraude

Se puede usar la API **REST** para enviar un texto, procesarlo y entregar el resultado de la metodología sin necesidad de usar la consola web o el dashboard para visualizar los resultados.

Antes de intentar consumir este servicio debe indicar en las cabeceras de la petición (**headers**) los parámetros de autenticación para identificarse ante el sistema. Use la llave **username** para indicar el nombre de usuario (con el mismo que inicia sesión en la interfaz web y **password** para indicar su contraseña.

Para esto, debe usar la URL con método **POST** https://demo.thefraudexplorer/rest/fraudTriangle o en caso de querer enviar varios mensajes en modo bulk https://demo.thefraudexplorer.com/rest/fraudTriangleBulk.

```
{
 "businessUnit" : "TECHNOLOGY",
 "application" : "Microsoft Word - My letter.docx",
 "phrases" : "Hola buenos dias, espero todo ande muy bien, escribo para contarte que estamos algo estresados en el area porque imaginate que un proveedor le hizo una propuesta de trabajo a uno de nuestros colaboradores y eso definitivamente representa una violacion a nuestro codigo de etica relacionada con conflictos de interes. Aqui todos dicen que cerremos la boca pero yo te estoy contando y lo quise eliminar, saludos.",
 "llmEngine" : "yes"
}
```

Esta consulta devolvería un resultado como:

```
{
   "pressureEvents": 1,
   "opportunityEvents": 3,
   "rationalizationEvents": 1,
   "suspiciousProbability": "91%",
   "messageTone": "neutral",
   "1stPersonPronouns": "yes",
   "criticalityFlag": "yes",
   "IntimityFlag": "no",
```

```
  "eventTopics": "information, suppliers",
  "eventClassification": "conocimiento, renuncia, negociaciones, ocultamiento, estres",
  "eventRisks": "concealment, psicosocial, suppliers",
  "llmResult": "suspicious",
  "phrasesMatched": {
    "pressureTerms": "estamos algo estresados",
    "opportunityTerms": "propuesta de trabajo, conflictos de interes, cerremos la boca",
    "rationalizationTerms": "quise eliminar"
  }
}
```


The Fraud Explorer es un software que junto con **FraudGPT** detecta el fraude y la corrupción en las organizaciones.

Correlación de eventos o workflows

Antes de intentar consumir este servicio debe indicar en las cabeceras de la petición (**headers**) los parámetros de autenticación para identificarse ante el sistema. Use la llave **username** para indicar el nombre de usuario (con el mismo que inicia sesión en la interfaz web y **password** para indicar su contraseña.

Algunas consultas deben tener las siguientes cabeceras. Más abajo en la tabla de operaciones se indican cuales de ellas son necesarias dependiendo de la operación.

Header	Valor	Explicación
page	1	Consultar pagina numero 1
size	100	Ventana de resultados por pagina
datefrom	2022-01-01	Rango de fecha "desde"
dateto	2022-02-28	Rango de fecha "hasta"

Para que el intercambio de datos entre el cliente y el servidor sea legible, use adicionalmente la cabecera **Content-Type** con el valor **application/json**.

Operación	Método	Headers	URL Ejemplo
Obtener el listado de los workflows	**GET**	**username, password, page, size**	https://url/rest/workFlows?list=all
Obtener los eventos de un workflow	**GET**	**username, password, page, size**	https://url/rest/workFlows?name=Compras

Un flujo de trabajo es aquel que permite generar alertas si se cumplen previamente unas condiciones de correlación de eventos. Los flujos de trabajo se crean en la plataforma administrativa de The Fraud Explorer.

The Fraud Explorer es un software que junto con **FraudGPT** detecta el fraude y la corrupción en las organizaciones.

Model Context Protocol

Antes de intentar consumir este servicio debe indicar en las cabeceras de la petición (**headers**) los parámetros de autenticación para identificarse ante el sistema. Use la llave **username** para indicar el nombre de usuario (con el mismo que inicia sesión en la interfaz web y **password** para indicar su contraseña.

Algunas consultas deben tener las siguientes cabeceras. Más abajo en la tabla de operaciones se indican cuales de ellas son necesarias dependiendo de la operación.

Header	Valor	Explicación
endpoint	jason_and716_agt	Identificación del endpoint
desde	2022-01-01	Rango de fecha "desde"
hasta	2022-02-28	Rango de fecha "hasta"

Las operaciones disponibles son:

Operación	Método	Headers	URL Ejemplo
Obtener el resumen general de las alertas	**GET**	**username, password, desde, hasta**	https://url/rest/mcp?general
Obtener una vista detallada de las alertas de un endpoint	**GET**	**username, password, endpoint, desde, hasta**	https://url/rest/mcp?detalle

Puede configurar su LLM para crear dos herramientas (tools) en Python que consuman este servicio API. Este script en Python implementa las dos herramientas (vista general y vista detallada de alertas):

```
from mcp.server.fastmcp import FastMCP
from datetime import datetime, timedelta
import httpx
import json

params = json.load(open('config.json'))

mcp = FastMCP("NOFRAUD")

#
```

```
# Descripcion de la herramienta: hace un resumen de todas las alertas que existen en un rango de fechas
#

@mcp.tool()
async def visionGeneral(desde: str, hasta: str) -> str:
    """
    Hace un resumen general de todas las alertas que existen en un rango de fechas.
    Esta herramienta solo se debe usar cuando se solicita un resumen general, no cuando se solicitan detalles.
    Cuando se solicitan detalles se debe usar la otra herramienta 'visionDetallada'.

    Estos son algunos ejemplos para usar esta herramienta:

    1. Podrias hacerme un resumen de las alertas desde el 1 de Abril al 30 de Abril de 2025?:
       visionGeneral(2025-04-01, 2025-04-30).
    2. Me podrias indicar si entre el periodo del 1 de Enero al 31 de Marzo de 2025 existieron alertas?:
       visionGeneral(2025-01-01, 2025-03-31).

    Requisitos para el uso de esta herramienta:

    1. La fecha de inicio debe ser anterior a la fecha de fin.
    2. Las fechas deben ser en formato YYYY-MM-DD.
    """
    global params
    async with httpx.AsyncClient() as client:
        url = params["url"] + "?general"
        headers = {
            "Content-Type": "application/json",
            "username": params["username"],
            "password": params["password"],
            "desde": str(desde),
            "hasta": str(hasta),
        }
        response = await client.get(url, headers=headers)
        response.raise_for_status()

    return response.json()

@mcp.tool()
async def visionDetallada(endpoint: str, desde: str, hasta: str) -> str:
    """
    Detalla las alertas que tiene un endpoint en especifico en un rango de fechas.
```

```
    Esta herramienta solo se debe usar cuando se solicitan detalles, no cuando se solicita un resumen.
    Cuando se solicita un resumen se debe usar la herramienta 'visionGeneral'.

    Estos son algunos ejemplos para usar esta herramienta:

    1. Podrias mostrarme las alertas del endpoint 'jhondoe' del 1 de Abril al 30 de Abril de 2025?:
       visionDetallada('jhondoe', 2025-04-01, 2025-04-30).
    2. Podrias detallarme las alertas del endpoint 'jhondoe@nofraud.la' del 1 de Enero al 31 de Marzo de 2025?:
       visionDetallada('jhondoe@nofraud.la', 2025-01-01, 2025-03-31).

    Requisitos para el uso de esta herramienta:

    1. El endpoint debe ser un nombre de usuario o un email. No se acepta 'todos' como endpoint.
    2. La fecha de inicio debe ser anterior a la fecha de fin.
    3. Las fechas deben ser en formato YYYY-MM-DD.
    """
    global params
    async with httpx.AsyncClient() as client:
        url = params["url"] + "?detalle"
        headers = {
            "Content-Type": "application/json",
            "username": params["username"],
            "password": params["password"],
            "endpoint": endpoint,
            "desde": str(desde),
            "hasta": str(hasta),
        }
        response = await client.get(url, headers=headers)
        response.raise_for_status()

    return response.json()

if __name__ == "__main__":
    mcp.run()
```

El archivo de configuración que debe crear según su instancia de The Fraud Explorer:

```
{
    "username": "mcp-username",
    "password": "su_password_mcp",
    "url": "https://demo.thefraudexplorer.com/rest/mcp"
```

```
}
```

The Fraud Explorer es un software que junto con **FraudGPT** detecta el fraude y la corrupción en las organizaciones

Ejemplos

Cómo se usa la API de The Fraud Explorer a través de varios ejemplos

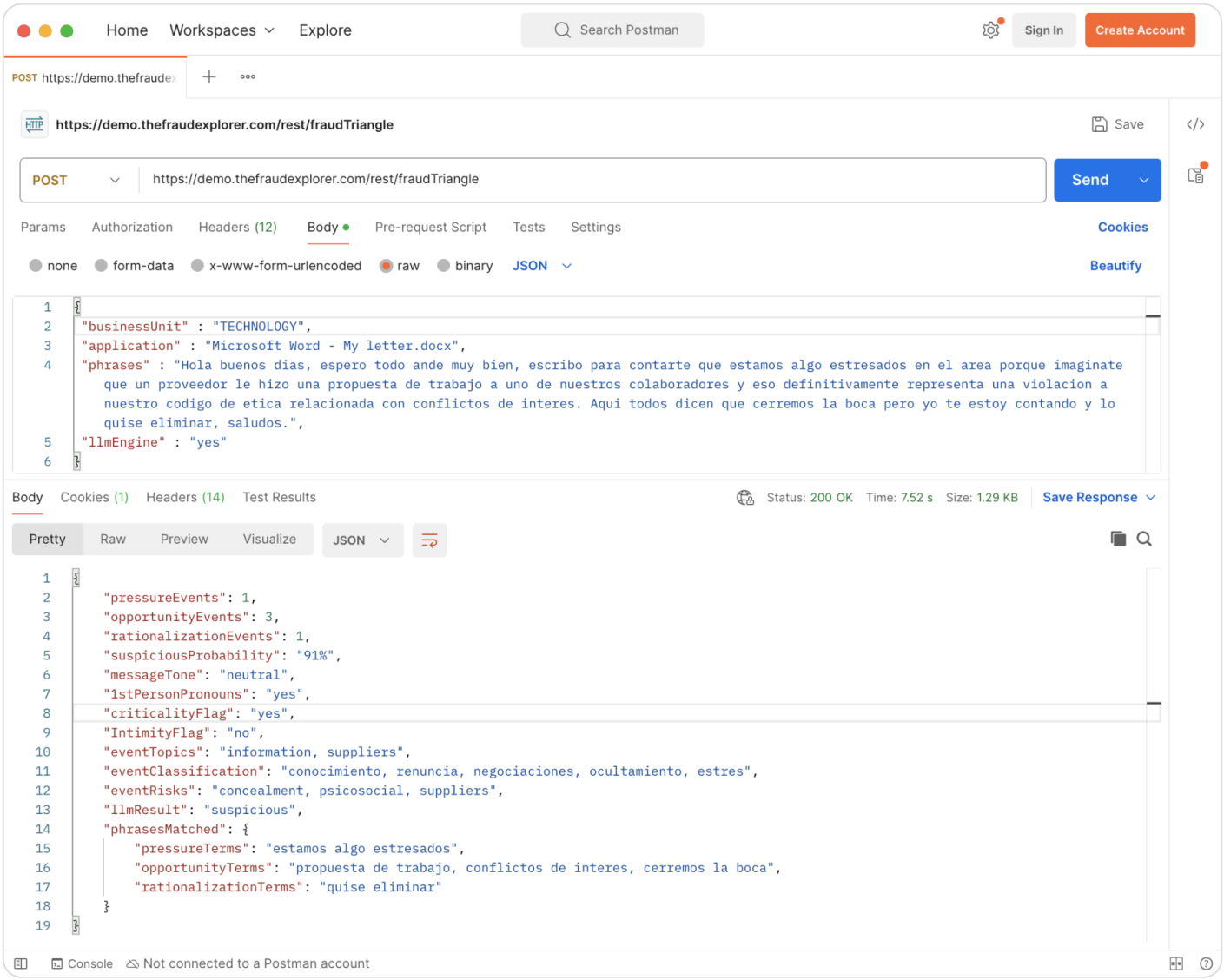
Insights del triángulo del fraude

En Postman cree una nueva nueva consulta, configure los headers **username**, **password** y **Content-Type** según la información de su instancia The Fraud Explorer.

Escriba en la URL la dirección https://suinstancia/rest/fraudTriangle, seleccione el método **POST** y luego en la pestaña **BODY** escriba:

```
{
 "businessUnit" : "TECHNOLOGY",
 "application" : "Microsoft Word - My letter.docx",
 "phrases" : "Hola buenos dias, espero todo ande muy bien, escribo para contarte que estamos algo estresados en el area porque imaginate que un proveedor le hizo una propuesta de trabajo a uno de nuestros colaboradores y eso definitivamente representa una violacion a nuestro codigo de etica relacionada con conflictos de interes. Aqui todos dicen que cerremos la boca pero yo te estoy contando y lo quise eliminar, saludos.",
 "llmEngine" : "yes"
}
```

Luego de clic en el botón **Send** y verá cómo retorna un análisis del contenido semántico:



Este servicio entrega información de la cantidad de comportamientos basados en el triángulo del fraude (presión, oportunidad y justificación), así como una probabilidad, acompañado de un análisis de tono y de intimidad.

Los insights también entregan información de valor agregado, como el análisis de pronombres personales (honestidad), detección de criticidad (alta o baja), un resumen de los tópicos del evento analizado, una clasificación de comportamientos, un inventario de riesgos y un match de frases en el contenido semántico.

The Fraud Explorer es un software que junto con **FraudGPT** detecta el fraude y la corrupción en las organizaciones.

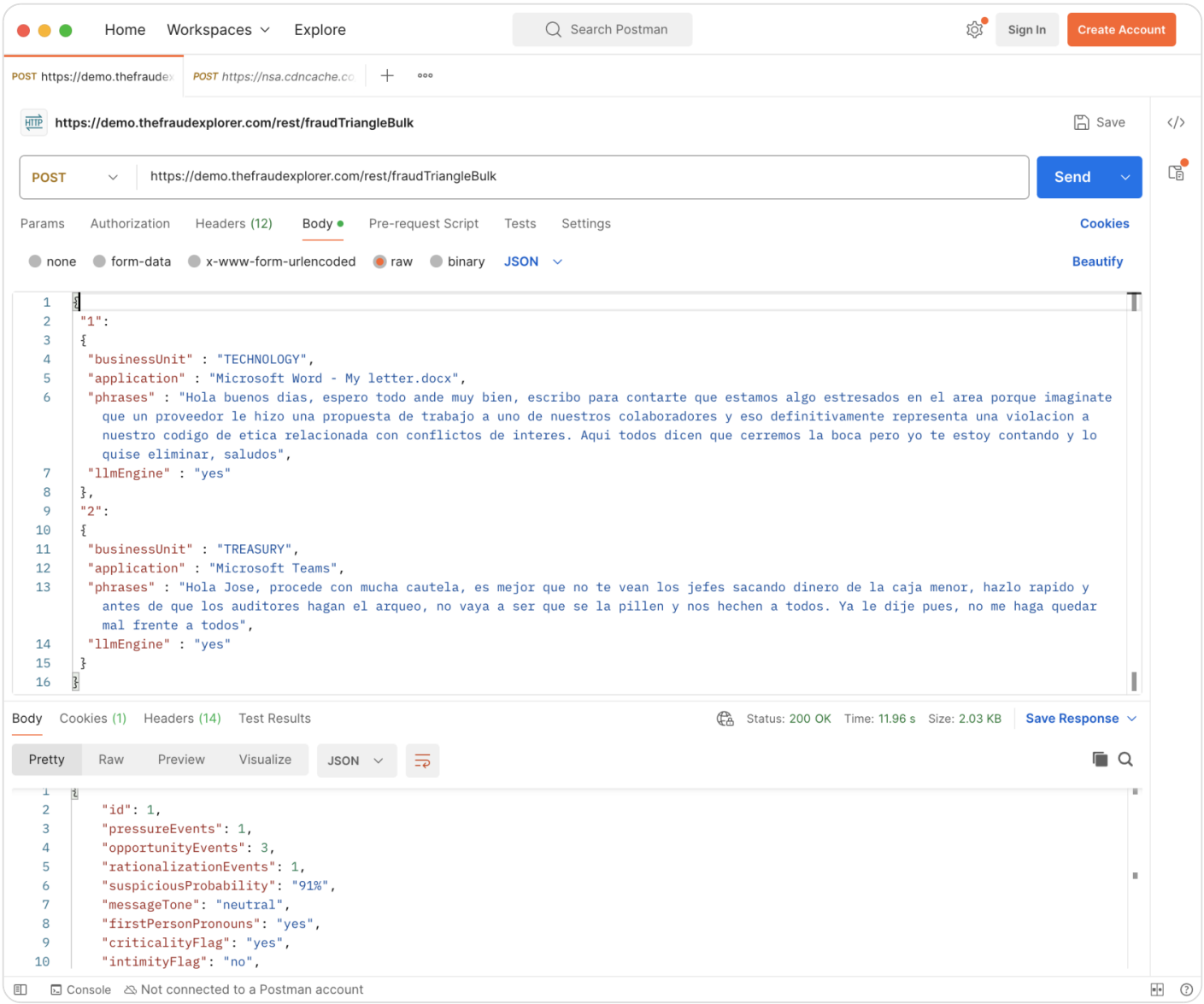
Modo Bulk para los insights

En Postman cree una nueva nueva consulta, configure los headers **username**, **password** y **Content-Type** según la información de su instancia The Fraud Explorer.

Escriba en la URL la dirección https://suinstancia/rest/fraudTriangleBulk, seleccione el método **POST** y luego en la pestaña **BODY** agregue cada evento de forma numérica así:

```
{
 "1":
 {
  "businessUnit" : "TECHNOLOGY",
  "application" : "Microsoft Word - My letter.docx",
  "phrases" : "Hola buenos dias, espero todo ande muy bien, escribo para contarte que estamos algo estresados en el area porque imaginate que un proveedor le hizo una propuesta de trabajo a uno de nuestros colaboradores y eso definitivamente representa una violacion a nuestro codigo de etica relacionada con conflictos de interes. Aqui todos dicen que cerremos la boca pero yo te estoy contando y lo quise eliminar, saludos",
  "llmEngine" : "yes"
 },
 "2":
 {
  "businessUnit" : "TREASURY",
  "application" : "Microsoft Teams",
  "phrases" : "Hola Jose, procede con mucha cautela, es mejor que no te vean los jefes sacando dinero de la caja menor, hazlo rapido y antes de que los auditores hagan el arqueo, no vaya a ser que se la pillen y nos hechen a todos. Ya le dije pues, no me haga quedar mal frente a todos",
  "llmEngine" : "yes"
 }
}
```

Luego de clic en el botón **Send** y verá cómo retorna un análisis del contenido semántico:



Este servicio en modo **BULK** entrega información de la cantidad de comportamientos basados en el triángulo del fraude (presión, oportunidad y justificación), así como una probabilidad, acompañado de un análisis de tono y de intimidad.

Los insights también entregan información de valor agregado, como el análisis de pronombres personales (honestidad), detección de criticidad (alta o baja), un resumen de los tópicos del evento analizado, una clasificación de comportamientos, un inventario de riesgos y un match de frases en el contenido semántico.

The Fraud Explorer es un software que junto con **FraudGPT** detecta el fraude y la corrupción en las organizaciones.

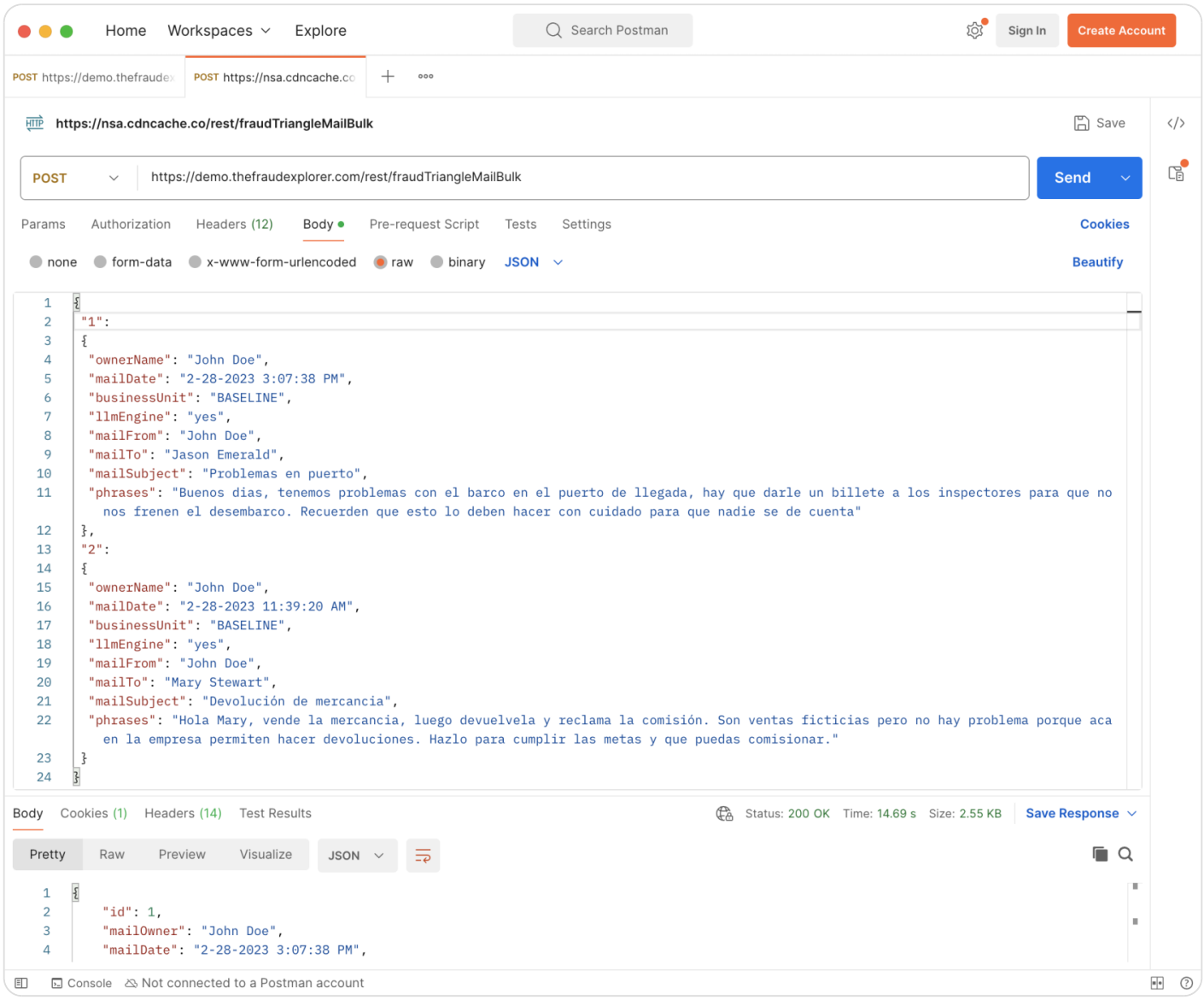
Modo Mail Bulk

En Postman cree una nueva nueva consulta, configure los headers **username**, **password** y **Content-Type** según la información de su instancia The Fraud Explorer.

Escriba en la URL la dirección https://suinstancia/rest/fraudTriangleMailBulk, seleccione el método **POST** y luego en la pestaña **BODY** agregue cada evento de forma numérica así:


```
{
 "1":
 {
  "ownerName": "John Doe",
  "mailDate": "2-28-2023 3:07:38 PM",
  "businessUnit": "BASELINE",
  "llmEngine": "yes",
  "mailFrom": "John Doe",
  "mailTo": "Jason Emerald",
  "mailSubject": "Problemas en puerto",
  "phrases": "Buenos dias, tenemos problemas con el barco en el puerto de llegada, hay que darle un billete a los inspectores para que no nos frenen el desembarco. Recuerden que esto lo deben hacer con cuidado para que nadie se de cuenta"
 },
 "2":
 {
  "ownerName": "John Doe",
  "mailDate": "2-28-2023 11:39:20 AM",
  "businessUnit": "BASELINE",
  "llmEngine": "yes",
  "mailFrom": "John Doe",
  "mailTo": "Mary Stewart",
  "mailSubject": "Devolución de mercancia",
  "phrases": "Hola Mary, vende la mercancia, luego devuelvela y reclama la comisión. Son ventas ficticias pero no hay problema porque aca en la empresa permiten hacer devoluciones. Hazlo para cumplir las metas y que puedas comisionar."
 }
}
```

Luego de clic en el botón **Send** y verá cómo retorna un análisis del contenido semántico:



Este servicio de **Mail** en modo **BULK** entrega información de la cantidad de comportamientos expresados en correos electrónicos basados en el triángulo del fraude (presión, oportunidad y justificación), así como una probabilidad, acompañado de un análisis de tono y de intimidad.

Los insights también entregan información de valor agregado, como el análisis de pronombres personales (honestidad), detección de criticidad (alta o baja), un resumen de los tópicos del evento analizado, una clasificación de comportamientos, un inventario de riesgos y un match de frases en el contenido semántico.

The Fraud Explorer es un software que junto con **FraudGPT** detecta el fraude y la corrupción en las organizaciones

Integraciones

The Fraud Explorer proporciona una API y varios servicios web que pueden ser usados para realizar integraciones con sistemas de terceros. En la siguiente tabla podrá ver un resumen de las integraciones que podría lograr con The Fraud Explorer:

Integración	**Escenario**
SIEM	The Fraud Explorer puede proporcionar alertas a un correlacionador de eventos para que éste tome en cuenta el valor de cada alerta para la toma de desiciones.
LLM	The Fraud Explorer proporciona herramientas compatibles con MCP (Model Context Protocol) que pueden ser integradas en un LLM para su consulta con la Inteligencia Artificial.
NAC	The Fraud Explorer puede integrarse con un NAC (Network Access Controller) para participar en el proceso de cuarentena de equipos aportando alertas reales de comportamientos deshonestos o anti éticos.
DLP	The Fraud Explorer puede servir como plugin para proporcionarle al DLP el input que necesita para el análisis semántico en busca de fuga de datos.
RPA	The Fraud Explorer puede ser consultado a través de sus API para incorporar su alertas en los flujos de automatización de procesos para detener o continuar operaciones.
SOC	The Fraud Explorer puede proporcionar al SOC de Ciberseguridad alertas relacionadas con la seguridad de la información o insider threats.

Estos son solamente algunos ejemplos en los cuales se puede usar una API para consultar los datos generados por The Fraud Explorer.

Casos de uso

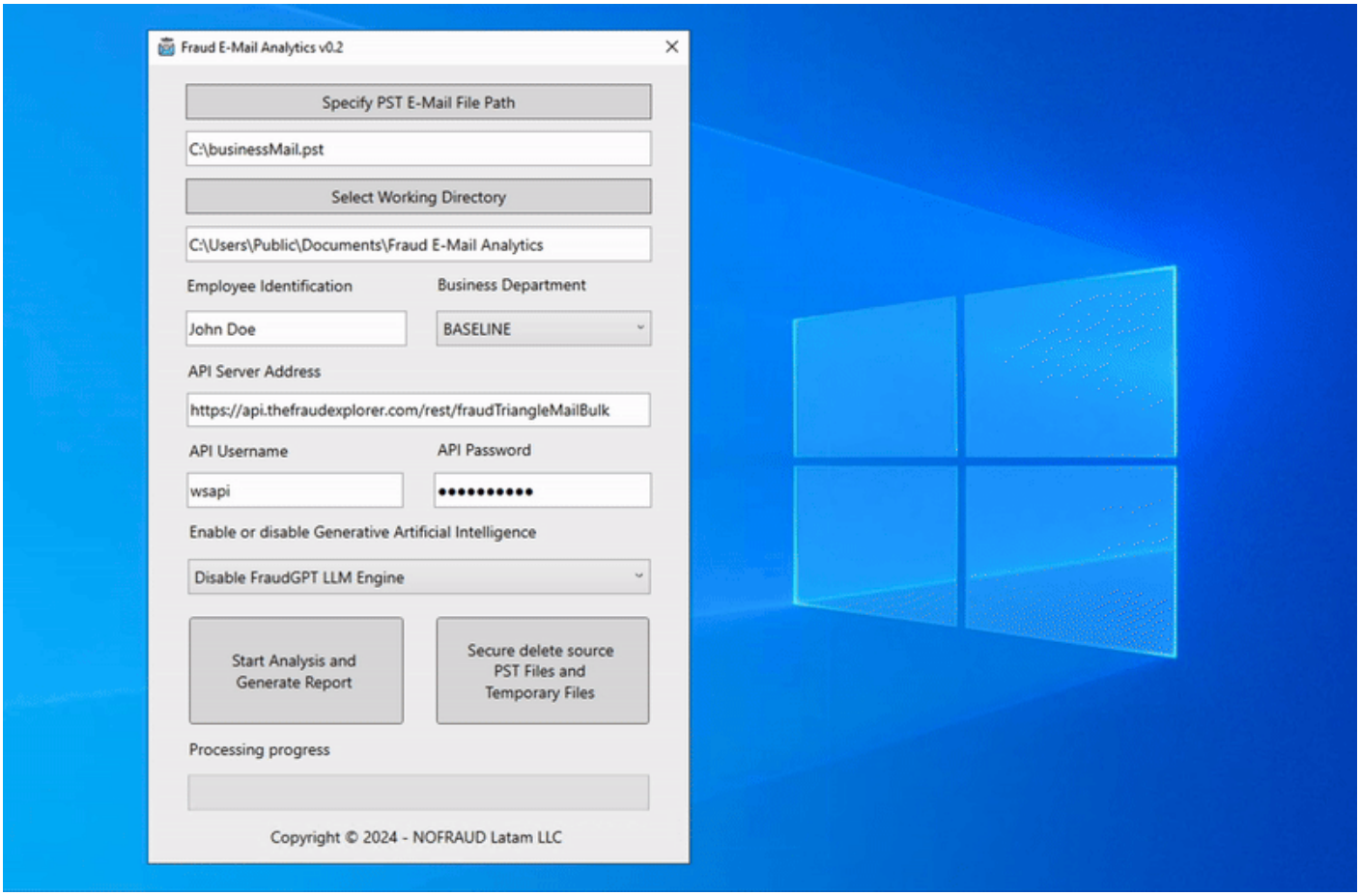
Diferentes implementaciones de API para casos cotidianos donde se quiere prevenir y detectar el fraude y la corrupción.

Casos de uso

Análisis de correos PST

Fraud E-Mail Analytics es un desarrollo de NOFRAUD que hace uso de la API **fraudTriangleMailBulk** con el objetivo de analizar los correos y chats alojados en un archivo PST con el algoritmo del triángulo del fraude y FraudGPT.

Una vez abierto, se selecciona el archivo PST, se especifica a qué persona pertenece el PST, el departamento al que fue asignado y al final se especifica si se quiere usar la IA Generativa Fraud GPT o no. Los datos del acceso a la API se cargan automáticamente y se componen de una URL, un usuario y password.



Una vez se tienen estos datos correctamente especificados, se procede a dar clic en **Start Analysis and Generate Report** y el software en ese momento realiza internamente las siguientes acciones:

1. **Crea un archivo de datos en Outlook:** el desarrollo de este software usa el SDK de Office, lo que significa que para que funcione, debe estar instalado Microsoft Office en el computador o servidor donde se ejecute este software. Lo que hace nuestro aplicativo es

usar un archivo de datos de Outlook para cargar allí el PST y poder ejecutar acciones programáticas sobre él.
2. **Extrae los items del PST:** programáticamente se empieza a recorrer el archivo PST extrayendo los items uno a uno y almacenándolos en un archivo local con formato JSON. Esta extracción va a permitir enviar los datos a la API, ya que la API solamente soporta el formato JSON.
3. **Envía los items en formato JSON a la API:** se cargan los items en modo BULK y se envían de manera cifrada a la API, la cual, recibe los datos, los procesa y por cada item genera un resultado basado en el algoritmo del triángulo del fraude.
4. **Recibe los datos de la API:** al terminar el procesamiento del lado del servidor, éste devuelve también en formato JSON los resultados, que son almacenados también en un archivo JSON de manera local ya preparados y formateados para la siguiente fase de generación del reporte.
5. **Genera un reporte en Excel:** se recorre el archivo JSON con los resultados de la API y se va llenando un archivo en Excel que previamente hemos creado como plantilla, con las alertas que el algoritmo del triángulo del fraude haya encontrado. Para este proceso, también se requiere el SDK de Microsoft Office.

Procesar un archivo PST de 1 GB puede tardar hasta 10 minutos para el algoritmo del triángulo del fraude y hasta 50 minutos si se activa la IA generativa FraudGPT.

The Fraud Explorer es un software que junto con **FraudGPT** detecta el fraude y la corrupción en las organizaciones.

Análisis de la voz en un IPPBX

The Fraud Explorer está en capacidad de procesar y hacer analítica del triángulo del fraude sobre conversaciones por voz a través de Asterisk. A continuación se mostrará cómo se realiza una prueba de concepto para ésta integración con la API.

Siga los pasos a continuación en Linux para realizar una instalación de Asterisk con el propósito de hacer la prueba de concepto. Si usted ya tiene un PBX operativo, sáltese esta sección y continúe con el procedimiento del DIALPLAN y la instalación del endpoint y el procesador ASR.

```
# yum -y groupinstall 'Development Tools'
# yum -y install libedit libedit-devel sox mpg123
# yum install wget ssh ncurses ncurses-devel uuid uuid-devel libuuid-devel jansson-devel libxml2-devel sqlite-devel
```

Descargue Asterisk y compílelo:

```
# cd ~
# wget http://downloads.asterisk.org/pub/telephony/asterisk/asterisk-17-current.tar.gz
# cd /usr/src
# tar zxvf ~/asterisk-17-current.tar.gz
# cd asterisk-17*
# ./configure --with-jansson-bundled
# make menuselect
# make
# make install
# make config
# make install-logrotate
# make samples
# systemctl enable asterisk
# systemctl restart asterisk
```

Configure el firewall para permitir conexiones TCP/UDP hacia el puerto 5060 de esta máquina virtual. Así mismo, redirija todo el tráfico RTP de los puertos UDP del 10000 al 20000 a esta máquina.

Descargue Google ASR para Asterisk y configúrelo en su PBX así:

```
# wget https://github.com/zaf/asterisk-speech-recog/tarball/master
# yum install flac flac-devel perl perl-JSON perl-libwww-perl.noarch perl-LWP-Protocol-https perl-Crypt-SSLeay
```

Copie el archivo **speech-recog.api** al directorio **/var/lib/asterisk/agi-bin** y establezca permisos de ejecución sobre el mismo. Configure ahora el DIALPLAN en el archivo **/etc/asterisk/extensions.conf** así:

```
[google-asr]
exten => 666,1,Answer();
same => n,agi(googletts.agi,"Hola, dime lo que sientes y termina con la tecla numeral",es);
same => n,agi(speech-recog.agi,es);
same => n,agi(googletts.agi, "Feliz dia, hasta luego",es);
same => n,Verbose(1,You said: ${utterance});
same => n,agi(thefraudexplorer.agi,"${utterance}");
same => n,Verbose(1,The Fraud Explorer status: ${ftaStatus});
same => n,Hangup();
```

En el archivo **/etc/asterisk/sip.conf** cree una extensión de prueba:

```
[100]
type=friend
secret=mysecret
username=100
callerid="benjamin@thefraudexplorer.com" <100>
host=dynamic
context=google-asr;
nat=force_rport,comedia
```

En el Google Cloud API habilite la característica **Google Cloud Speech API**. Copie su API Key y péguela en el archivo de configuración **/var/lib/asterisk/agi-bin/speech-recog.agi** en la variable **key**. Descargue luego el motor TTS de Google, descomprímalo y copie el archivo **googletts.agi** al directorio **/var/lib/asterisk/agi-bin.**

Ingrese a la plataforma web de The Fraud Explorer y entre al módulo de generación de endpoints. Allí seleccione **Asterisk VoIP PBX**, estableciendo la dirección del servidor y las credenciales API REST. Al descargar, copie el archivo resultante generado **thefraudexplorer.agi** y cópielo a la carpeta **/var/lib/asterisk/agi-bin/**.

Así luce el código que implementa la API

Este código usa la API **endPoint?query=phrases&id=agentID** para el envío de datos semánticos. Debe ajustar al final del archivo los datos de conexión a la API, como usuario, contraseña y otros datos propios de la instancia, como las llaves de cifrado.

```
<?php

/*
 * This function encrypts string with AES-128 bits
 *
 * @param string $unencrypted -> text to cipher
 * @param string $cipherkey -> cipher key
 *
 * return : encrypted string
*/

function encRijndael($unencrypted, $cipherkey)
{
    $key = $cipherkey;
    $iv = $cipherkey;
    $iv_utf = mb_convert_encoding($iv, 'UTF-8');
    $toreturn = mcrypt_encrypt(MCRYPT_RIJNDAEL_128, $key, $unencrypted, MCRYPT_MODE_CBC, $iv_utf);
    $toreturn = base64_encode($toreturn);

    return $toreturn;
}

/*
 * This function decrypts string with AES-128 bits
 *
 * @param string $encrypted -> text to decrypt
 * @param string $cipherkey -> cipher key
 *
 * return : decrypted string
*/

function decRijndael($encrypted, $cipherkey)
{
    $encrypted = rawurldecode($encrypted);
    $key = $cipherkey;
    $iv = $cipherkey;
    $iv_utf = mb_convert_encoding($iv, 'UTF-8');
```

```
    $toreturn = mcrypt_decrypt(MCRYPT_RIJNDAEL_128, $key, base64_decode(str_replace("_","/",str_replace("-","+",$encrypted))), MCRYPT_MODE_CBC, $iv_utf);
    $toreturn = filter_var($toreturn, FILTER_SANITIZE_STRING, FILTER_FLAG_STRIP_LOW);
    return $toreturn;
}

/*
 * This function heartbeats endpoint
 *
 * @param string $agentID -> endpoint ID
 * @param string $serverTFE -> server address
 * @param string $agentVersion -> agent version
 * @param string $keyPass -> server password
 * @param string $domain -> endpoint domain
 * @param string $cipherKey -> cipher key
 *
 * return : void function
*/

function reportOnline($agentID, $serverTFE, $agentVersion, $keyPass, $domain, $cipherKey)
{
    $rawURL = $serverTFE."/update.php";
    $pbxVersion = shell_exec("/sbin/asterisk -rx \"core show version\" | grep \"Asterisk\" | awk '{ print $2 }'");
    $pbxVersion = trim(preg_replace('/\s+/', '', $pbxVersion));
    $unwanted_chars = array('+'=>'-', '/'=>'_');
    $params = "";

    $getRequest = array(
        'token' => encRijndael($agentID, $cipherKey),
        's' => encRijndael($pbxVersion, $cipherKey),
        'v' => encRijndael($agentVersion, $cipherKey),
        'k' => encRijndael($keyPass, $cipherKey),
        'd' => encRijndael($domain, $cipherKey)
    );

    foreach($getRequest as $key=>$value) $params .= $key.'='.$value.'&';

    $params = trim($params, '&');
    $params = strtr($params, $unwanted_chars);
    $ch = curl_init();
```

```
    curl_setopt($ch, CURLOPT_URL, $rawURL.'?'.$params );
    curl_setopt($ch, CURLOPT_RETURNTRANSFER, 1);
    curl_setopt($ch, CURLOPT_CONNECTTIMEOUT, 60);
    curl_setopt($ch, CURLOPT_USERAGENT, "Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)");
    curl_setopt($ch, CURLOPT_HEADER, 0);

    $result = curl_exec($ch);
    curl_close($ch);
}

/*
 * This function sanitizes string for unwanted characters
 *
 * @param string $rawPhrase -> string to sanitize
 *
 * return : sanitized string
*/

function phraseSanitization($rawPhrase)
{
    $unwanted_chars = array('Š'=>'S', 'š'=>'s', 'Ž'=>'Z', 'ž'=>'z', 'À'=>'A', 'Á'=>'A', 'Â'=>'A', 'Ã'=>'A', 'Ä'=>'A',
'Å'=>'A', 'Æ'=>'A', 'Ç'=>'C',
    'È'=>'E', 'É'=>'E', 'Ê'=>'E', 'Ë'=>'E', 'Ì'=>'I', 'Í'=>'I', 'Î'=>'I', 'Ï'=>'I', 'Ñ'=>'N', 'Ò'=>'O', 'Ó'=>'O', 'Ô'=>'O',
'Õ'=>'O', 'Ö'=>'O',
    'Ø'=>'O', 'Ù'=>'U', 'Ú'=>'U', 'Û'=>'U', 'Ü'=>'U', 'Ý'=>'Y', 'Þ'=>'B', 'ß'=>'Ss', 'à'=>'a', 'á'=>'a', 'â'=>'a',
'ã'=>'a', 'ä'=>'a', 'å'=>'a',
    'æ'=>'a', 'ç'=>'c', 'è'=>'e', 'é'=>'e', 'ê'=>'e', 'ë'=>'e', 'ì'=>'i', 'í'=>'i', 'î'=>'i', 'ï'=>'i', 'ð'=>'o', 'ñ'=>'n',
'ò'=>'o', 'ó'=>'o',
    'ô'=>'o', 'õ'=>'o', 'ö'=>'o', 'ø'=>'o', 'ù'=>'u', 'ú'=>'u', 'û'=>'u', 'ý'=>'y', 'þ'=>'b', 'ÿ'=>'y');

    $sanitizedPhrase = strtr($rawPhrase, $unwanted_chars);
    $sanitizedPhrase = strtolower($sanitizedPhrase);

    return $sanitizedPhrase;
}

/*
 * This function sends data (words) to the server
 *
```

```
 * @param string $serverTFE -> server address
 * @param string $agentId -> endpoint ID
 * @param string $restUser -> REST username
 * @param string $restPass -> REST password
 * @param string $ipAddress -> endpoint IP address
 * @param string $domain -> endpoint company domain
 * @param string $callWith -> call with extension
 * @param string $phrases -> paragraph
 *
 * return : void function
*/

function sendData($serverTFE, $agentId, $restUser, $restPass, $ipAddress, $domain, $callWith, $phrases)
{
    $serverAddress = $serverTFE."/rest/endPoints?query=phrases&id=".$agentId;
    $APIuser = $restUser;
    $APIpass = $restPass;

    $postRequest = array(
        'hostPrivateIP' => $ipAddress,
        'userDomain' => $domain,
        'appTitle' => $callWith,
        'phrases' => $phrases
    );

    $payload = json_encode($postRequest);

    $ch = curl_init();
    curl_setopt($ch, CURLOPT_URL, $serverAddress);
    curl_setopt($ch, CURLOPT_POST, 1);
    curl_setopt($ch, CURLOPT_POSTFIELDS, $payload);
    curl_setopt($ch, CURLOPT_RETURNTRANSFER, true);

    $headers = [
    'username: ' .$APIuser,
    'password: ' .$APIpass,
    'Content-Type: application/json',
    ];

    curl_setopt($ch, CURLOPT_HTTPHEADER, $headers);
```

```
    $server_output = curl_exec($ch);
    curl_close ($ch);
}

/*
 * This function reads server remote commands
 *
 * @param string $serverTFE -> server address
 * @param string $cipherKey -> cipher key
 *
 * return : command status
*/

function collectionPhraseStatus($serverTFE, $cipherKey)
{
   $xml = simplexml_load_file($serverTFE.'/update.xml');
   $phraseCollectionStatus = decRijndael($xml->token[0]['arg'], $cipherKey);

   if ($phraseCollectionStatus == "textAnalytics 1") $phraseStatus = "enabled";
   else $phraseStatus = "disabled";

   return $phraseStatus;
}

/* PBX internal variables */

$agivars = array();

while (!feof(STDIN))
{
    $agivar = trim(fgets(STDIN));

    if ($agivar === '') break;

    $agivar = explode(':', $agivar);
    $agivars[$agivar[0]] = trim($agivar[1]);
}

extract($agivars);
```

```
/* PBX Endpoint variables */

$serverTFE = "https://demo.thefraudexplorer.com";
$keyPass = "31173";
$cipherKey = "yourkeyandiv";
$restUser = "apirestuser";
$restPass = "apirestpassword";
$agentVersion = "0.1";
$ipAddress = shell_exec("/sbin/asterisk -rx \"sip show peers\" | grep \"".$agi_callerid."/".$agi_callerid."\" | awk '{
print $2 }'");
$ipAddress = trim(preg_replace('/\s+/', '', $ipAddress));
$callerName = $agi_calleridname;
$callerNameArray = explode("@", $callerName);
$domain = $callerNameArray[1];
$name = $callerNameArray[0];
$agentId = $name."_".$agi_callerid."1kc9_pbx";
$callWith = "Phone call with ".$agi_dnid;
$phrases = phraseSanitization($argv[1]);

/* Exit if no phrase */

if ($phrases == "" || collectionPhraseStatus($serverTFE, $cipherKey) == "disabled")
{
    echo "SET VARIABLE ftaStatus no-sent";
    exit;
}

/* Create or update endpoint and send data */

reportOnline($agentId, $serverTFE, $agentVersion, $keyPass, $domain, $cipherKey);
sendData($serverTFE, $agentId, $restUser, $restPass, $ipAddress, $domain, $callWith, $phrases);

/* Finish AGI */

echo "SET VARIABLE ftaStatus sent-ok";

?>
```

Instale un Softphone

Descargue Bria para iOS o Android y registre la extensión 100. Cuando registre, llame al número "666" y escuchará una voz que le pide decirle "como se siente". Hable y exprese lo que siente, al finalizar presione la tecla **#** y luego visualice la consola **The Fraud Explorer** en busca de eventos alertas sobre las frases dichas.

Configuración en producción

Para su sistema en producción, debe instalar el motor de Google ASR y TTS junto con el AGI de **The Fraud Explorer** y usar el módulo **ChanSpy**, para capturar el audio de una llamada en vivo y posteriormente pasar su transcripción a The Fraud Explorer. El único requisito que debe respetar es el contar con una buena identificación de las personas que están conectadas a la planta, a través del Caller ID y el User Name, puesto que de esta manera se identificarán los usuarios en la plataforma de analítica.