Monta la NSA en tu casa

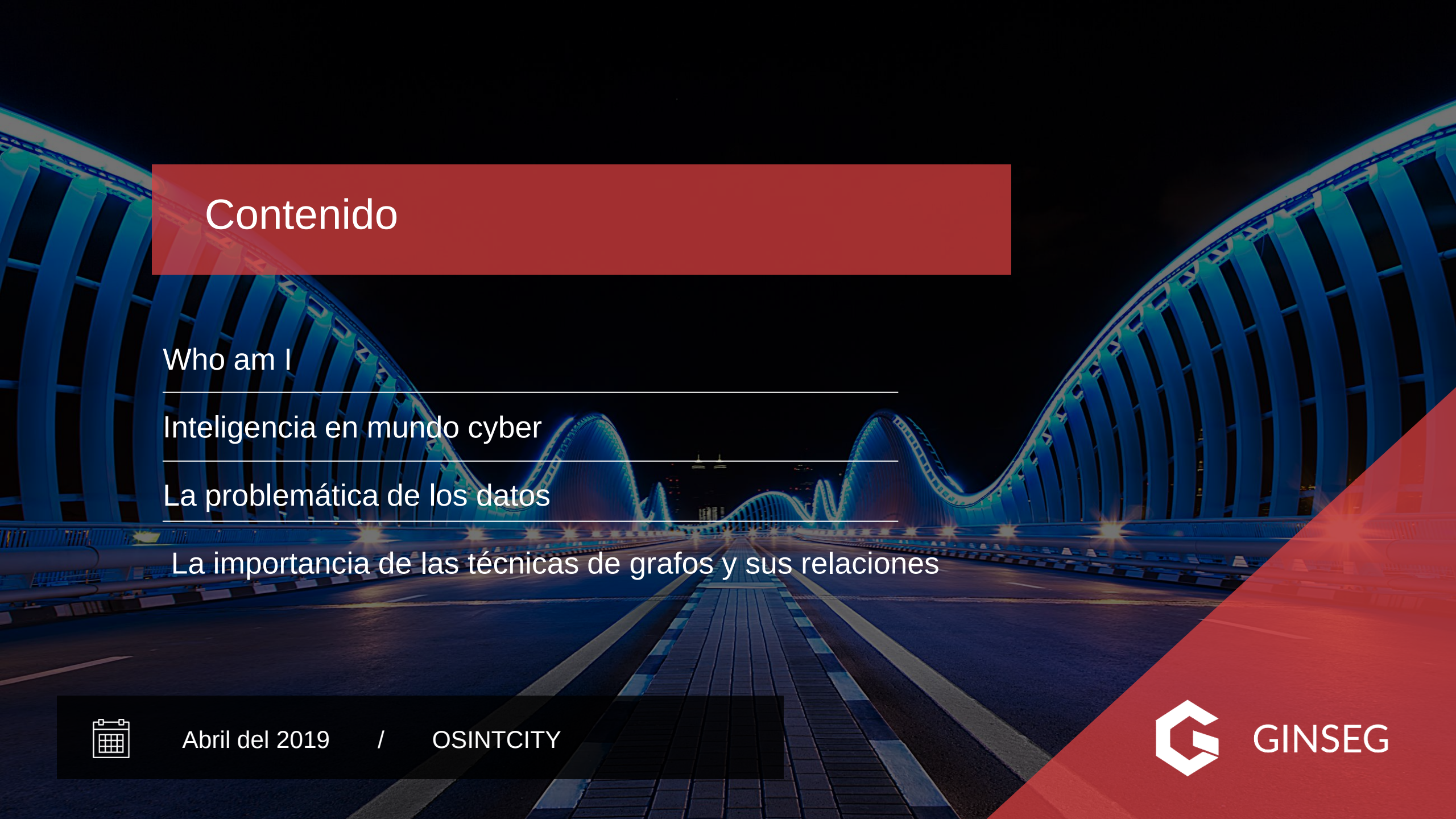
Inteligencia aplicada al mundo cyber

Inteligencia

Ciberseguridad

OSINT CITY

GINSEG
Inteligencia y ciberseguridad



Contenido

Who am I

Inteligencia en mundo cyber

La problemática de los datos

La importancia de las técnicas de grafos y sus relaciones

Abril del 2019 / OSINTCITY

GINSEG

GINSEG

Iván Portillo

Ciberinteligencia & Seguridad

Analista Senior – Big4

ivanportillomorales

ivanPorMor

Wiktor Nykiel

Ingeniero de Ciberseguridad

Sector Financiero

wiktornykiel

WiktorNykiel

Inteligencia en mundo cyber

Explorando un objetivo con OSINT

Como encaja la inteligencia, ciberinteligencia y OSINT

Problemas a los que OSINT proporciona soluciones

Ciclo de Inteligencia aplicado a ciberinteligencia

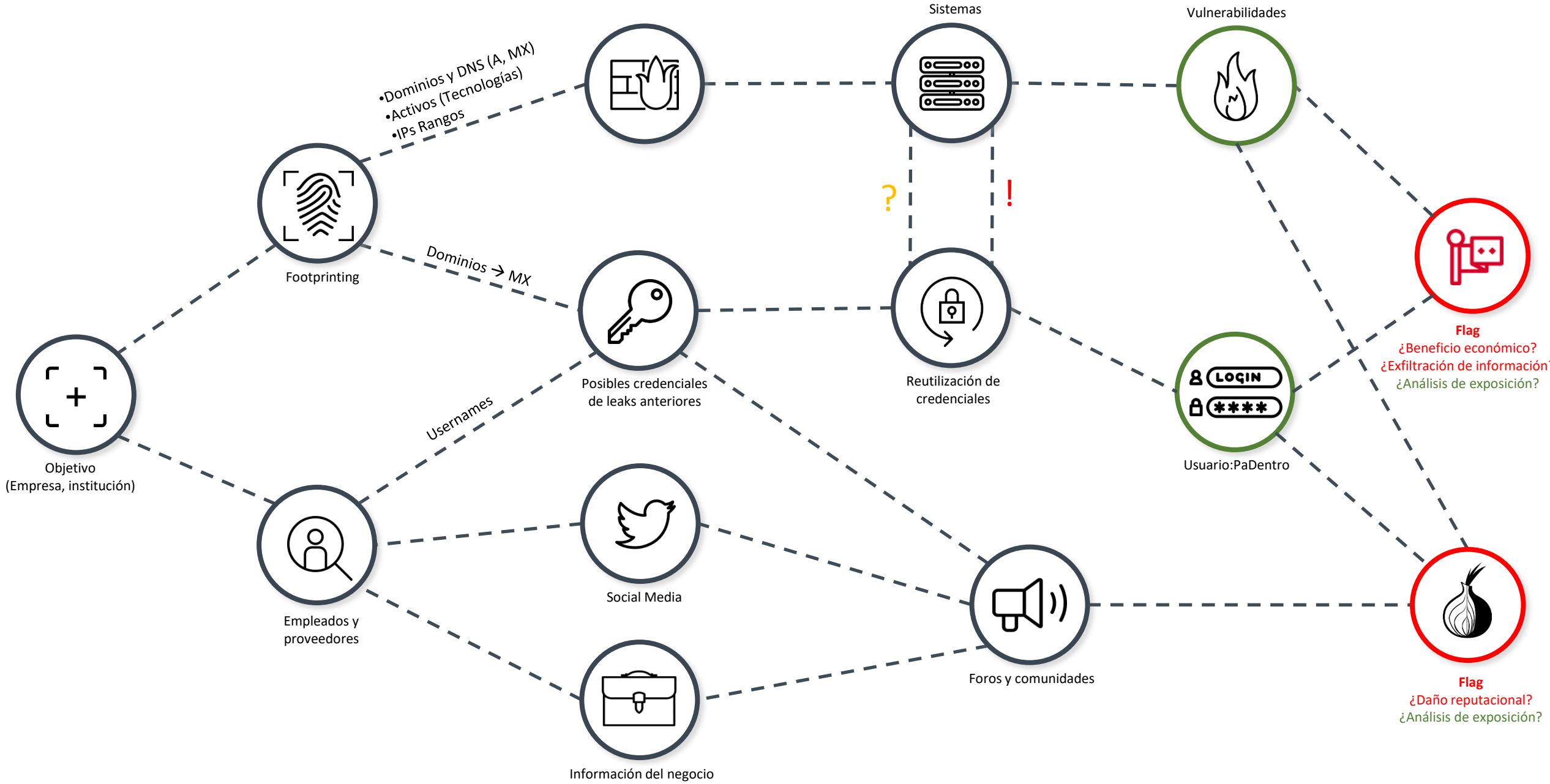
Interlocutores

Abril del 2019 / OSINTCITY

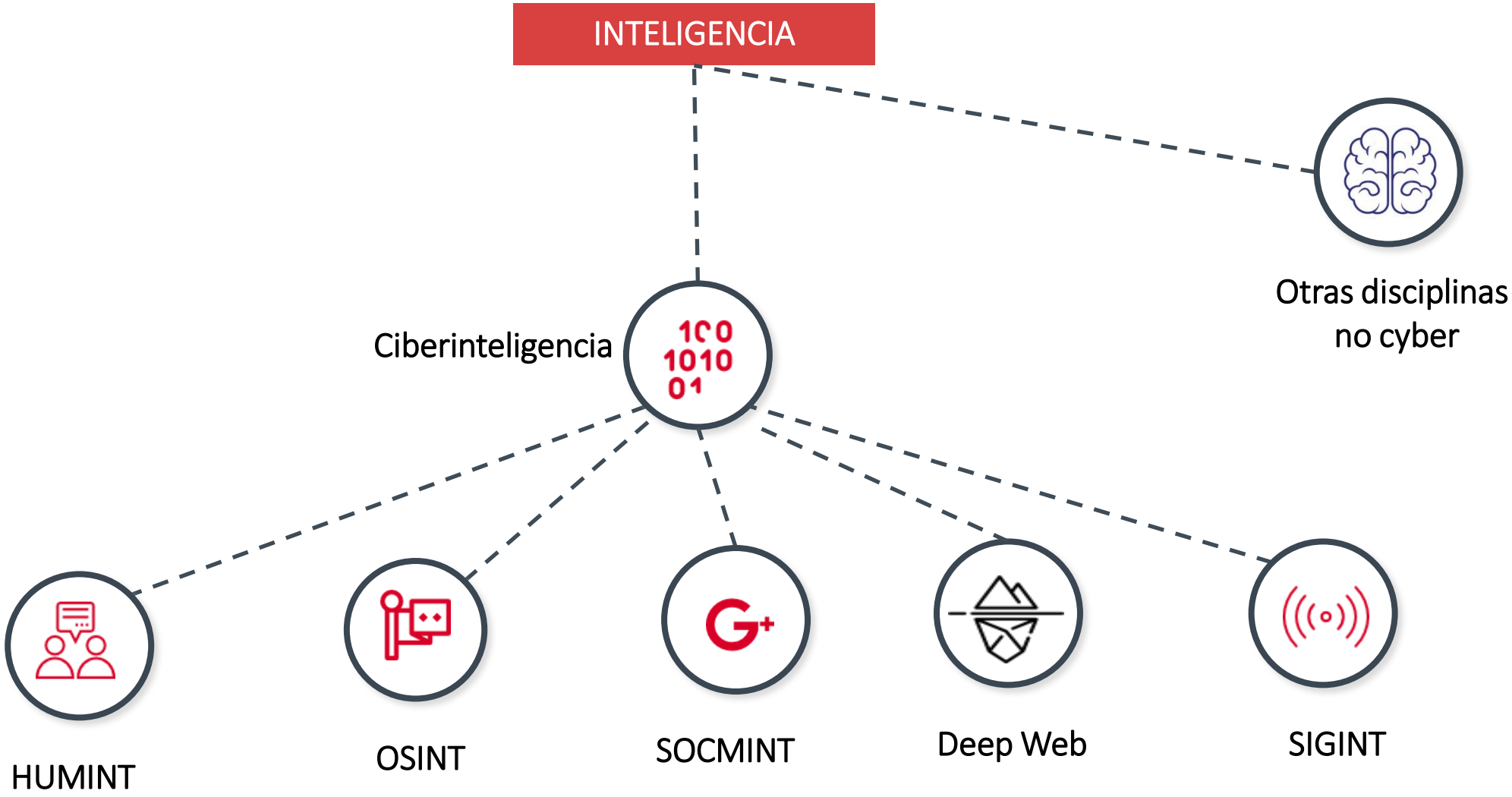
GINSEG

Explorando un objetivo con OSINT

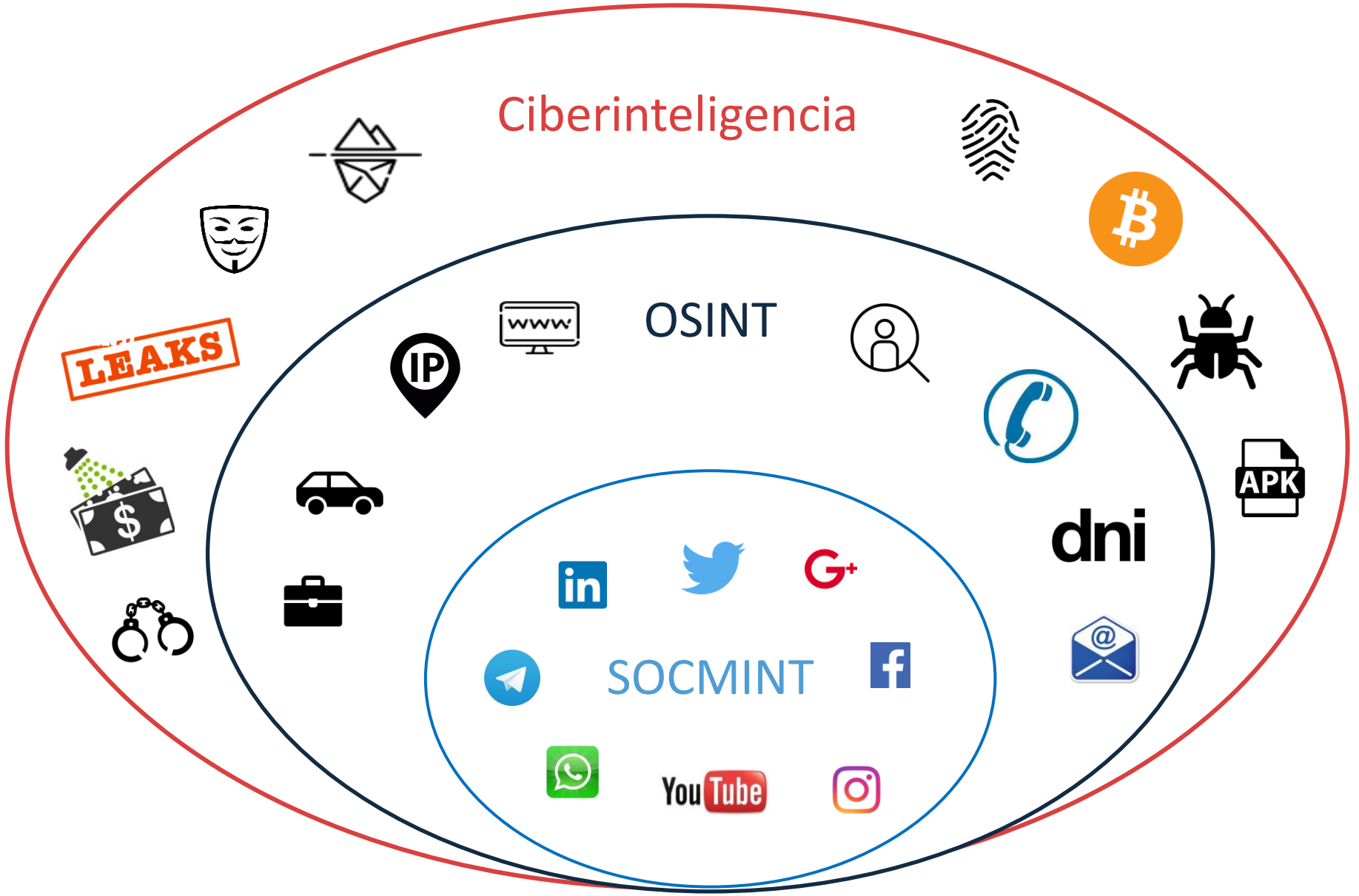
GINSEG



Como encaja la inteligencia, ciberinteligencia y OSINT



Como encaja la inteligencia, ciberinteligencia y OSINT



Problemas a los que OSINT proporciona soluciones

GINSEG

Ámbito		
Personal	Profesional	Corporativo
• Protección ante el robo de credenciales. • Presencia en Bases de Datos. • Exposición de Datos Personales. • Avisos de multas • Seguimiento de menciones • Marca personal • Búsqueda de piso (idealista/censo – m2 reales) • Búsqueda de trabajo • Compras online / verificación de comercios online	• Posicionamiento laboral • Alineamiento con los requisitos profesionales • Estudios de mercado • Marca personal • Top trends industria / materia • Comparativa de salarios • Mejores empresas / empleos / localizaciones para trabajar	• Análisis de exposición • Menciones en medios digitales • Reputación y marca • Suplantación de marca • Cybersquatting • Amenazas físicas • Malware dirigido • Perdidas económicas • Ventajas competitivas • Exfiltración de información

Ciclo de Inteligencia aplicado a ciberinteligencia

- Identificar necesidades del destinatario
- Estrategias a aplicar
- Fijar objetivo y alcance.
- Planificación de proyecto

Externo

- Recopilación de información de amenazas
- Agregar y consolidar datos
- Casos de uso de operaciones de seguridad

Interno

- Datos de incidentes y eventos empresariales
- Controlar brechas y vulnerabilidades
- Datos de activos críticos

- Correlación de tendencias
- **Identificar información de valor.**
  - Objetivo de la amenaza
  - Perfil de la amenaza
  - TTPs
  - Vector de ataque
  - Árbol de ataque
  - Actor
- Evaluar y **priorizar el riesgo**.
- Elaborar **producto de inteligencia**

- Entrega de producto de inteligencia a destinatario para que pueda tomar decisiones.
- Retroalimentación con Fase 1.

Interlocutores

GINSEG

Información relevante que se convierte en inteligencia a través de un **ciclo dinámico de colección, análisis, integración y producción.**

Esta **inteligencia** puede ser **consumida** por los **equipos de seguridad** así como por **altos cargos**.

Estratégico

Es **información de alto nivel**. Es poco probable que sea técnico y puede abarcar aspectos como el **impacto financiero** de la actividad cibernética, las **tendencias de ataque** y las áreas que pueden afectar las **decisiones comerciales** de alto nivel.

- Junta directiva / CEO.
- Otros altos responsables en la toma de decisiones.

Operacional

Es información sobre ataques específicos que llegan a la organización.

- Personal de seguridad y defensa.

Táctico

Tácticas, técnicas y procedimientos (TTP, por sus siglas en inglés) es información sobre cómo los actores pretenden o están realizando sus ataques.

- CISOs, DPO, CTO & Security Architects.

Técnico

Se trata de datos o información sobre indicadores de sucesos específicos. La inteligencia de amenaza técnica generalmente alimenta las funciones de investigación o supervisión de una empresa.

- Analistas, SOCs, IR, SysAdmins. e IT Staff.

La problemática de los datos

Abril del 2019 / OSINTCITY

GINSEG

Problemática con datos generados

GINSEG

Datos extraídos de fuentes OSINT necesitan contexto

danger.rulez.sk/projects/bruteforceblocker/blist.php

```
128.199.137.145  # 2019-04-04 16:53:08  5  1600432
134.209.28.22    # 2019-04-17 01:36:46  5  1606229
192.81.215.71    # 2019-04-13 17:10:14  5  1605042
205.185.120.250  # 2019-04-15 10:07:37  5  1605470
167.99.208.22    # 2019-04-17 19:17:41  5  1606203
68.183.39.84     # 2019-04-08 19:05:30  5  1601638
95.163.138.230   # 2019-04-18 17:12:29  5  1600641
37.49.228.121    # 2019-04-13 01:41:54  5  1602470
180.150.127.191  # 2019-04-11 08:04:26  5  1602818
116.77.132.129   # 2019-04-19 17:44:52  5  1601339
165.227.114.95   # 2019-04-23 00:18:23  5  1608258
164.132.135.199  # 2019-04-24 15:38:53  5  1608418
185.60.133.243   # 2019-04-14 19:03:53  5  1604556
116.110.220.87   # 2019-04-08 00:29:12  5  1601851
103.210.133.20   # 2019-04-23 03:27:59  5  1599875
37.59.111.193    # 2019-04-24 10:57:44  4  1604241
178.62.211.171   # 2019-04-15 11:37:47  4  1606142
37.182.236.14    # 2019-04-14 14:05:22  4  1601578
139.11.81.103    # 2019-04-21 04:48:28  4  1600788
```

osint.bambenekconsulting.com/feeds/c2-dommasterlist.txt

```
actionmaster.net,Domain used by pizd,2019-04-24 18:11,http://osint.bambenekcons
angrypeople.net,Domain used by pizd,2019-04-24 18:11,http://osint.bambenekconsu
battlepeople.net,Domain used by pizd,2019-04-24 18:11,http://osint.bambenekcons
becausefamous.net,Domain used by pizd,2019-04-24 18:11,http://osint.bambenekcon
becomefamous.net,Domain used by pizd,2019-04-24 18:11,http://osint.bambenekcons
chargeforward.net,Domain used by pizd,2019-04-24 18:11,http://osint.bambenekcon
chargemaster.net,Domain used by pizd,2019-04-24 18:11,http://osint.bambenekcons
cleanforward.net,Domain used by pizd,2019-04-24 18:11,http://osint.bambenekcons
cleanindustry.net,Domain used by pizd,2019-04-24 18:11,http://osint.bambenekcon
cleanpeople.net,Domain used by pizd,2019-04-24 18:11,http://osint.bambenekconsu
clearforward.net,Domain used by pizd,2019-04-24 18:11,http://osint.bambenekcons
clearlanguage.net,Domain used by pizd,2019-04-24 18:11,http://osint.bambenekcon
clearpeople.net,Domain used by pizd,2019-04-24 18:11,http://osint.bambenekconsu
collegeneither.net,Domain used by pizd,2019-04-24 18:11,http://osint.bambenekco
cornerpeople.net,Domain used by pizd,2019-04-24 18:11,http://osint.bambenekconsulting.com/manual/pizd.txt
countryneedle.net,Domain used by pizd,2019-04-24 18:11,http://osint.bambenekconsulting.com/manual/pizd.txt
3b0dnm1tg4gm2ogolt1lbuwgxm.com,Domain used by GOZ,2019-04-24 18:00,http://osint.bambenekconsulting.com/manual/goz
17a4m976mysmj1w0yzw7cdnhpq.com,Domain used by GOZ,2019-04-24 18:00,http://osint.bambenekconsulting.com/manual/goz
182384x1knzacq11gop9q1xkxasy.com,Domain used by GOZ,2019-04-24 18:00,http://osint.bambenekconsulting.com/manual/g
caaksa.com,Domain used by pykspa,2019-04-24 18:07,http://osint.bambenekconsulting.com/manual/pykspa.txt
cealis.net,Domain used by pykspa,2019-04-24 18:07,http://osint.bambenekconsulting.com/manual/pykspa.txt
fcvwvcw.info,Domain used by pykspa,2019-04-24 18:07,http://osint.bambenekconsulting.com/manual/pykspa.txt
fhvhse.info,Domain used by pykspa,2019-04-24 18:07,http://osint.bambenekconsulting.com/manual/pykspa.txt
ilpsjyverx.info,Domain used by pykspa,2019-04-24 18:07,http://osint.bambenekconsulting.com/manual/pykspa.txt
ivqvrodsholapet.com,Domain used by pykspa,2019-04-24 18:07,http://osint.bambenekconsulting.com/manual/pykspa.txt
ivzhfqfidv.info,Domain used by pykspa,2019-04-24 18:07,http://osint.bambenekconsulting.com/manual/pykspa.txt
kckspkdsholapet.com,Domain used by pykspa,2019-04-24 18:07,http://osint.bambenekconsulting.com/manual/pykspa.txt
```

#totalhash

Malware Analysis Database

HOME | SEARCH | **NETWORK SEARCH** | UPLOAD | API ACCESS | BROWSE | ABOUT US | HELP

Search #totalhash For Network Matches

Keys: av dnsrr email filename hash ip mutex pdb registry url useragent version

av:Gen*Heur.BrResMon.1 — Search

Here you can search for static or dynamic characteristics of samples in our database

Switch to **Normal View**

Displaying 1 - 20 of 11013 results

SHA1	TIMESTAMP	DNSRR	IP
3f6c73119acbb4517baabe17d6088570a3554b45	2018-05-25 14:04:42		2018-05-25 14:04:42
2bc02e47e92bce7799a9c3183c391d8df9a3b64f	2018-05-25 04:08:06		2018-05-25 04:08:06
4f0f9b32983510940bc14e1d58ff609766b1506b	2018-05-25 00:41:41		2018-05-25 00:41:41
de7450b8834ba230a9393ebe304fac1b61947af0	2018-05-24 10:08:54		2018-05-24 10:08:54
51f1cf725c47f43e705e2a5f6c990c082e2319b6	2018-05-23 20:52:32		2018-05-23 20:52:32
fcaa83c6524a43002a0229d874bc5a26b2fac90d	2018-05-23 05:09:31		
06e4c6364f2624cdc26e59c385bc6b2e83508fd1	2018-05-22 00:45:30		
86f42c0e3636567451218115088681 92dc148e98	2018-05-21 20:19:03		
e62c32b52d0c78e7e6a1e44f6ab7cea591ca70ca	2018-05-21 16:09:42		

https://lists.blocklist.de/lists/all.txt

```
1.85.36.90
1.85.7.26
1.9.138.178
1.9.21.100
1.9.46.177
100.24.52.144
100.35.242.84
100.38.16.101
100.7.53.104
101.109.15.118
101.12.236.183
101.17.111.205
101.178.122.50
101.187.249.26
101.207.113.73
101.227.64.169
101.227.90.171
101.228.143.176
101.229.96.25
101.230.223.158
101.231.104.82
101.231.125.54
101.231.140.218
101.236.29.126
101.236.33.85
101.251.196.14
101.251.197.238
101.251.245.124
101.251.245.220
101.255.40.130
101.255.52.171
101.255.64.194
101.255.64.58
101.255.65.139
```

Problemática con datos generados

Datos extraídos de herramientas de ciberinteligencia

PASTEBIN

pipl

ZoomEye

FOFA

SHODAN
Computer Search Engine

MALTEGO

spiderfoot

';--have i been pwned?

DataSploit

censys

robtex

ThreatCrowd

tinfoleak

CYMON.IO

HYBRID ANALYSIS

OpenDNS

Namech_k

PASSIVE TOTAL
BUILT FOR ANALYSTS BY ANALYSTS

VirusTotal

hunter

DOMAINTOOLS

Problemática con datos generados

GINSEG

Información extraída de fuentes de datos

Información extraída de Plataformas de Inteligencia de Amenazas (TIP – Threat Intelligence Platforms)

Múltiples fuentes y formatos

GINSEG

Fuentes

+

Agregación de datos

Online pastes	xBLs	STIX / TAXII
Honeynets	Spam blacklists	IoC
Trapmails	Safe browsing	Malware
Online trackers	Cybersquatting	Botnets / C&C
Referers	APK Markets	Social Media
BBDDs antivirus	TOR crawler	BBDDs threat intelligence
CERTs	Hidden IRC	

Agregación de todas las fuentes

Enriquecimiento de los datos

Filtrado

Categorización

Entrega →

Multiples formatos para compartir

- Collective Intelligence Framework (CIF).
- Cyber Observable eXpression (CybOX).
- Incident Object Description and Exchange Format (IODEF).
- Open Indicators of Compromise (OpenIOC).
- Open Threat Exchange (OTX).
- Structured Threat Information Expression (STIX).
- Trusted Automated eXchange of Indicator Information (TAXII).
- Vocabulary for Event Recording and

Operacional | Técnico | Táctico

La importancia de las técnicas de grafos

Abril del 2019 / OSINTCITY

GINSEG

GINSEG

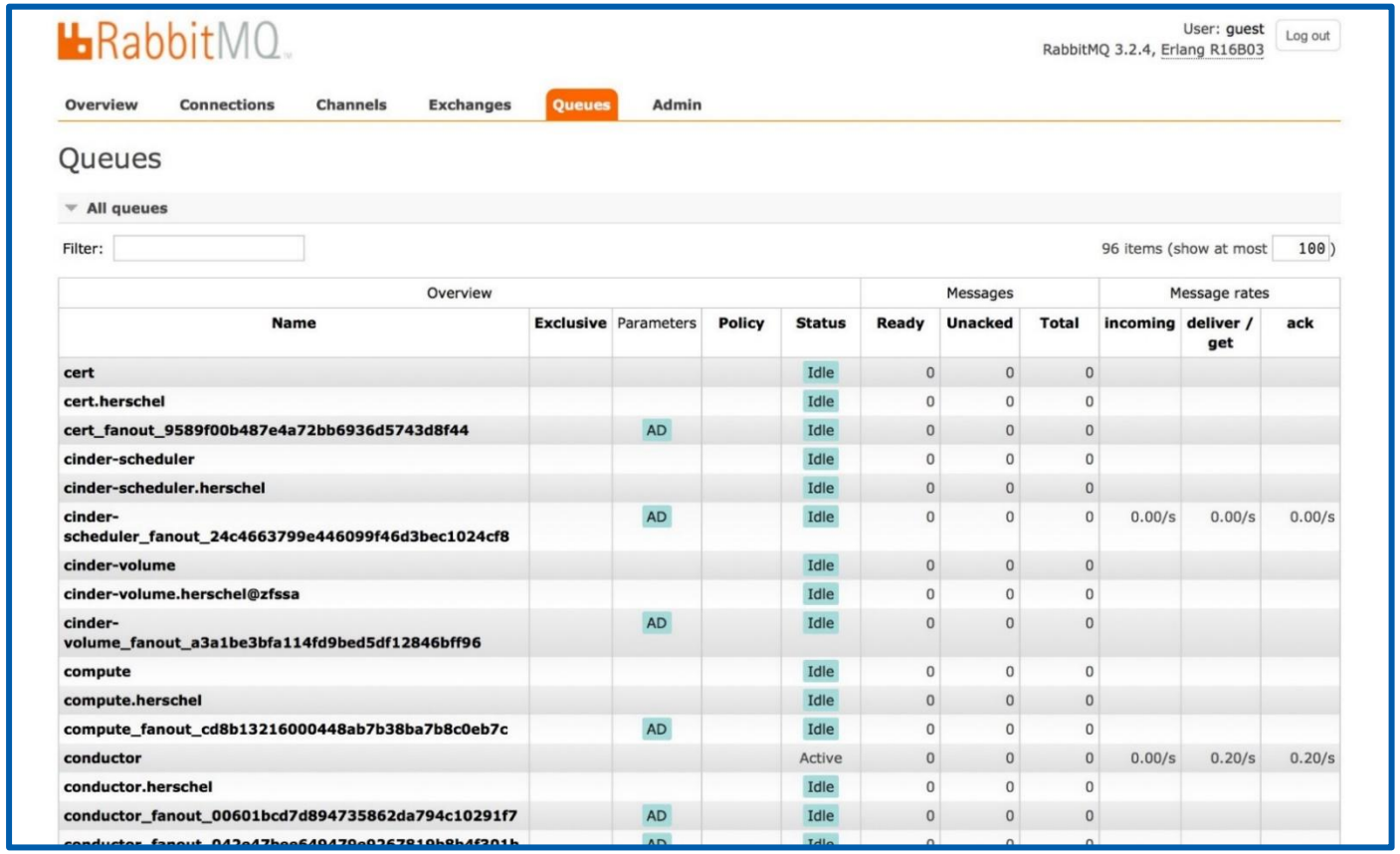
RabbitMQ

¿Qué es?

- Gestor de colas de mensajes para comunicar la información entre diferentes sistemas, aplicaciones, etc.
- Software Libre y compatible con diferentes protocolos de mensajería.

¿Qué Ofrece?

- Alta Disponibilidad.
- Garantía de entrega.
- Escalabilidad.
- Distribución de mensajes a múltiples destinatarios.
- Ordena y prioriza tareas.
- Balanceo de carga de trabajo.



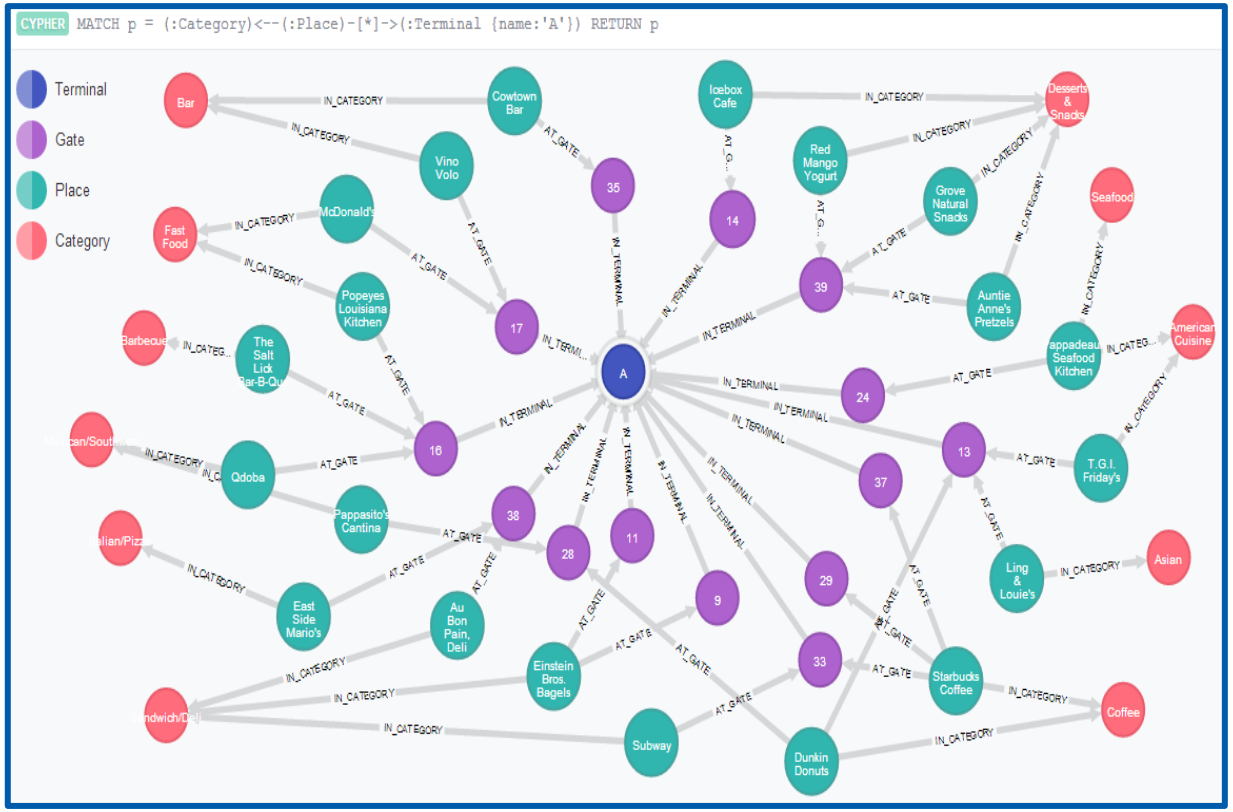
Overview					Messages			Message rates		
Name	Exclusive	Parameters	Policy	Status	Ready	Unacked	Total	incoming	deliver / get	ack
cert				Idle	0	0	0			
cert.herschel				Idle	0	0	0			
cert_fanout_9589f00b487e4a72bb6936d5743d8f44		AD		Idle	0	0	0			
cinder-scheduler				Idle	0	0	0			
cinder-scheduler.herschel				Idle	0	0	0			
cinder-scheduler_fanout_24c4663799e446099f46d3bec1024cf8		AD		Idle	0	0	0	0.00/s	0.00/s	0.00/s
cinder-volume				Idle	0	0	0			
cinder-volume.herschel@zfssa				Idle	0	0	0			
cinder-volume_fanout_a3a1be3bfa114fd9bed5df12846bff96		AD		Idle	0	0	0			
compute				Idle	0	0	0			
compute.herschel				Idle	0	0	0			
compute_fanout_cd8b13216000448ab7b38ba7b8c0eb7c		AD		Idle	0	0	0			
conductor				Active	0	0	0	0.00/s	0.20/s	0.20/s
conductor.herschel				Idle	0	0	0			
conductor_fanout_00601bcd7d894735862da794c10291f7		AD		Idle	0	0	0			

Creando nodos y relaciones

GINSEG

¿Qué es?

- Es una base de datos orientada a grafos, que permite obtener relaciones entre diferentes nodos.
- Dispone de versión Community y versión de pago.



¿Qué ofrece?

- Soporta transacciones ACID (Atomicidad, Consistencia, Aislamiento, Durabilidad).
- Agilidad para gestionar grandes cantidades de datos.
- Flexibilidad y escalabilidad.
- Alta disponibilidad y Balanceo de carga.

Preparando la infraestructura

GINSEG

docker-compose.yml

```yaml
neo4j:
  image: neo4j:3.5.0
  hostname: "neo4j"
  environment:
  #- NEO4J_HOST=192.168.18.136
  - NEO4J_AUTH=neo4j/password
  - NEO4J_apoc_import_file_enabled=true
  - NEO4J_apoc_export_file_enabled=true
  - NEO4J_apoc_import_file_use__neo4j__config=true
  - NEO4J_dbms_connector_http_listen__address=0.0.0.0:7474
  - NEO4J_dbms_connector_https_listen__address=0.0.0.0:6477
  - NEO4J_dbms_connector_bolt_listen__address=0.0.0.0:7687
  - NEO4J_dbms_connectors_default_listen__address=127.0.0.1
  - NEO4J_dbms_security_procedures_unrestricted=apoc.*
  ports:
  - "7474:7474"
  - "7473:7473"
  - "7687:7687"
  volumes:
  - ./dataNeo4j:/data
  - ./NEOplugins:/plugins


rabbit1:
  image: "rabbitmq:3-management"
  hostname: "rabbit"
  environment:
   RABBITMQ_DEFAULT_USER: "admin"
   RABBITMQ_DEFAULT_PASS: "password"
   RABBITMQ_DEFAULT_VHOST: "/"
  ports:
    - "15672:15672"
    - "5672:5672"
```

Infraestructura por servicio con Docker

Ubicación

./orquestación/orquestación/arquitectura_orquestación/docker-compose.yml

Comando sudo docker-compose up –d

Configuración NEO4J

- URL: http://127.0.0.1:7474
- Connect URL: bolt://127.0.0.1:7687
- User: neo4j
- Password: password

Configuración RabbitMQ

- URL: http://127.0.0.1:15672
- User: admin
- Password: password

Preparando la infraestructura

GINSEG

start_arquitectura.sh

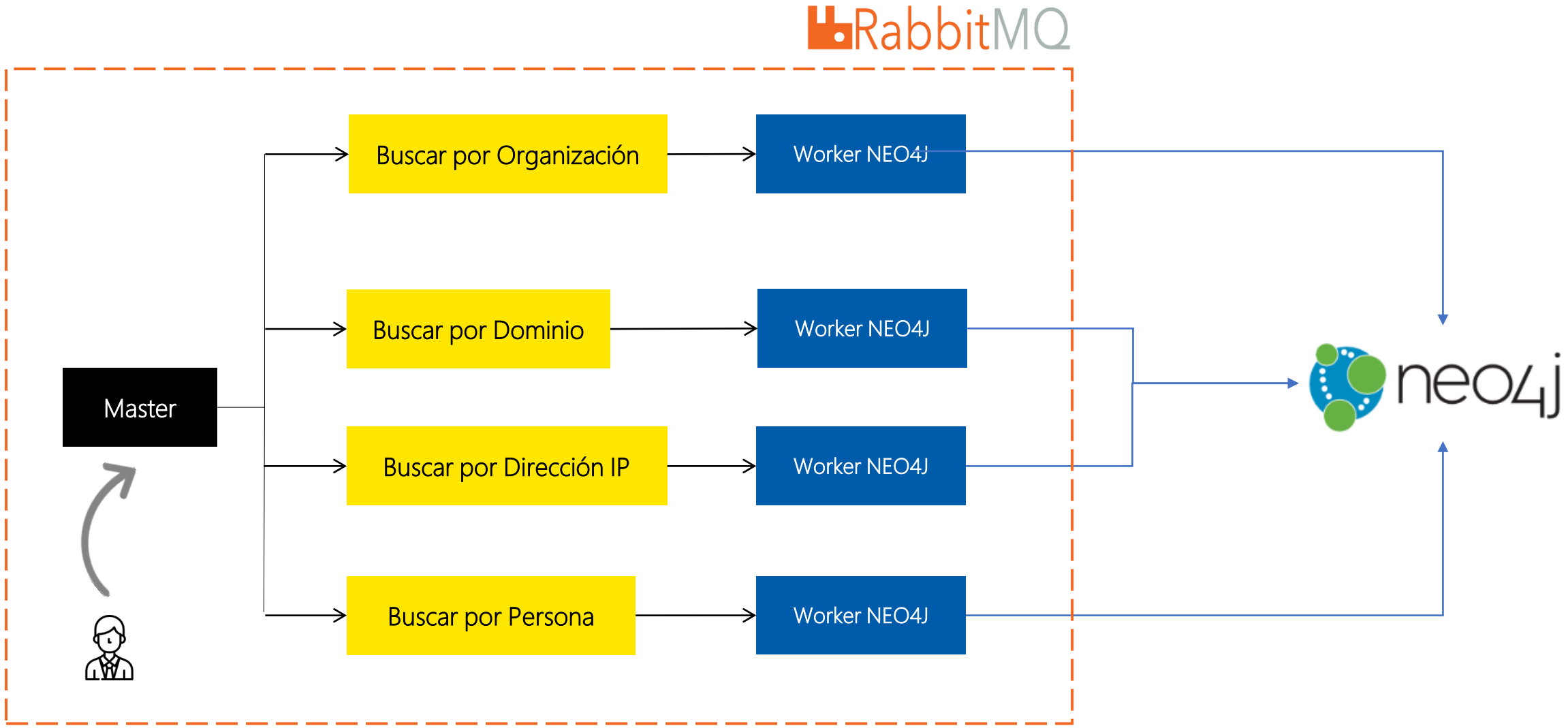
```
#@creator Ivan Portillo
#!/bin/sh

#ejecutar dockers de NEO4J y RabbitMQ

echo -e "\nKilling Dockers..."
cd ./arquitectura_orquestacion/
sudo docker-compose down
echo -e "\nRunning Dockers..."
sleep 10
sudo docker-compose up -d


#Instalando dependencias.
while true; do
    read -p "Do you want to install dependencies? (yes/no)" result;
    case $result in
        "yes")
            echo -e "\nInstalling Dependencies.."
            cd ..
            pip install -r requirements.txt
            break;;

        "no") break;;
        *) echo "Invalid option $REPLY"

    esac
done
```

Ejecución de Infraestructura

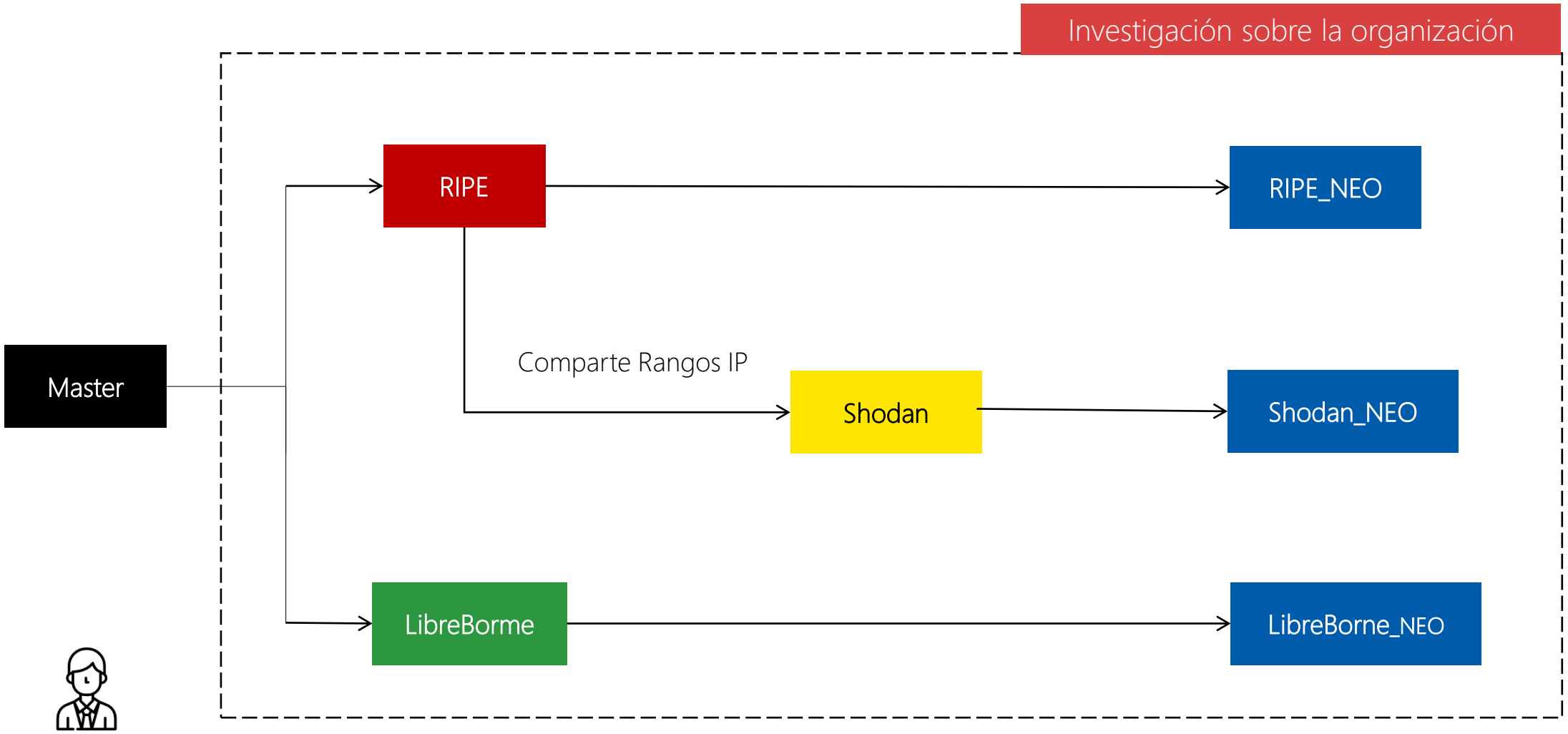
Ubicación ./orquestación/orquestación/

Comando sh start_arquitectura.sh

Orquestación de Herramientas relacionando datos – Mapa Global

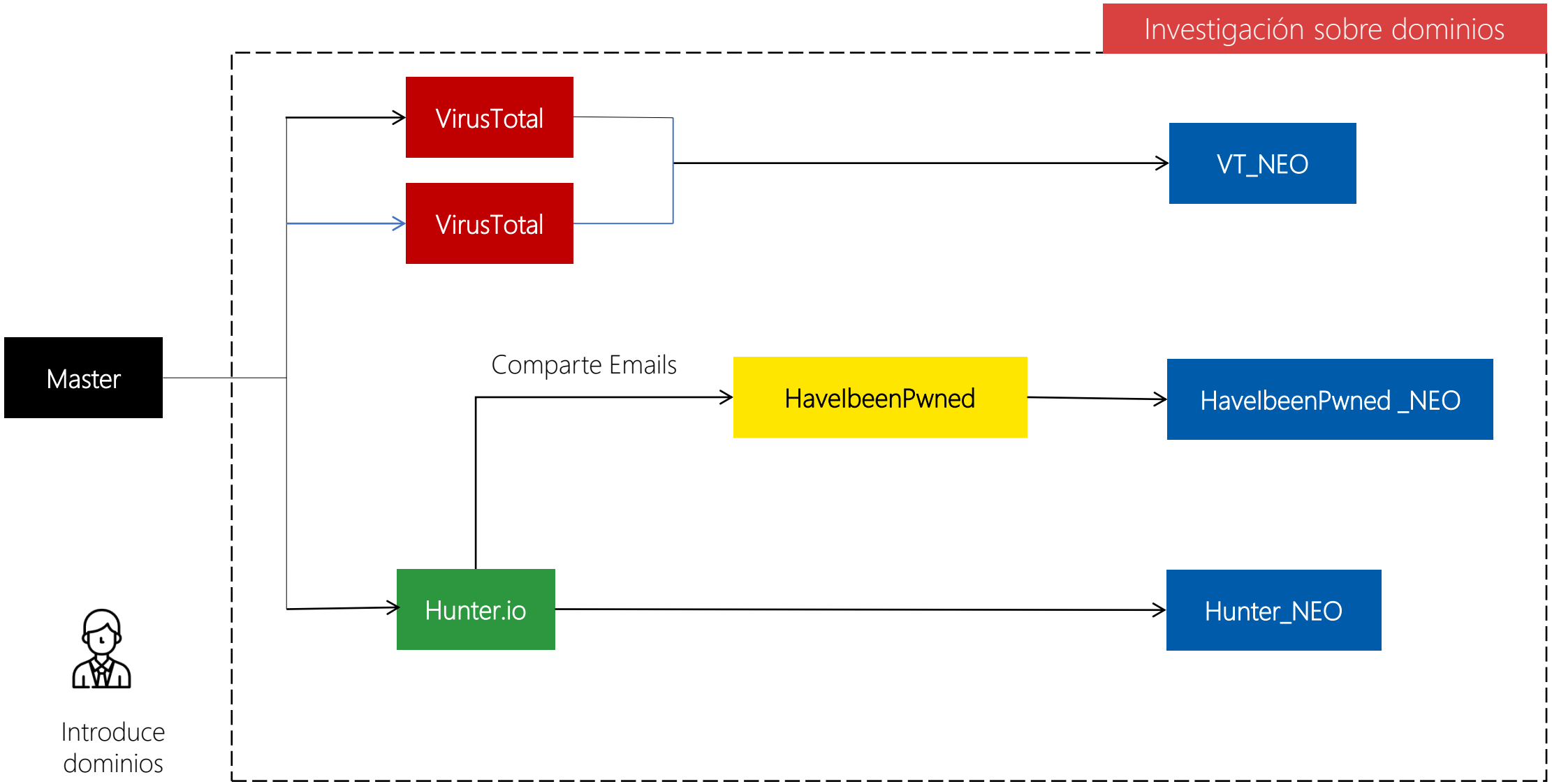


Orquestación de Herramientas relacionando datos



Introduce organizaciones

Orquestación de Herramientas relacionando datos



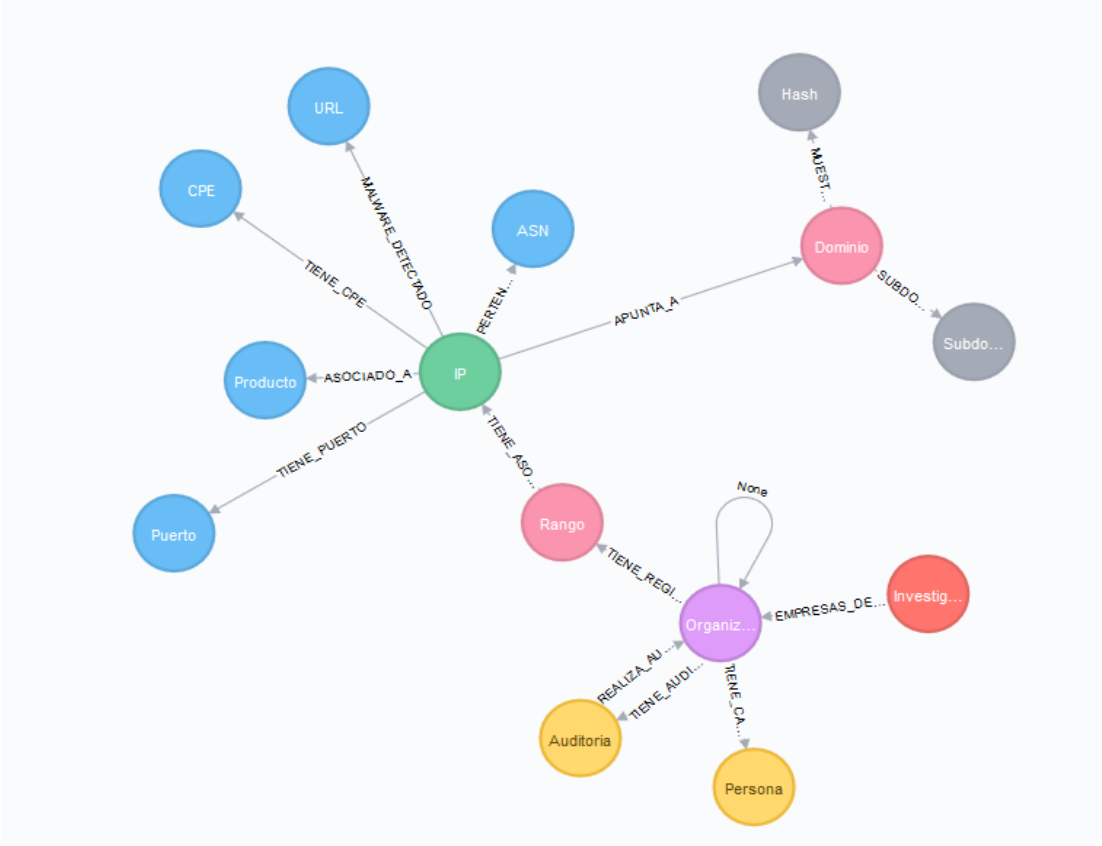
Orquestación de Herramientas relacionando datos

GINSEG

Comando NEO4J para grafo de nodos y relaciones

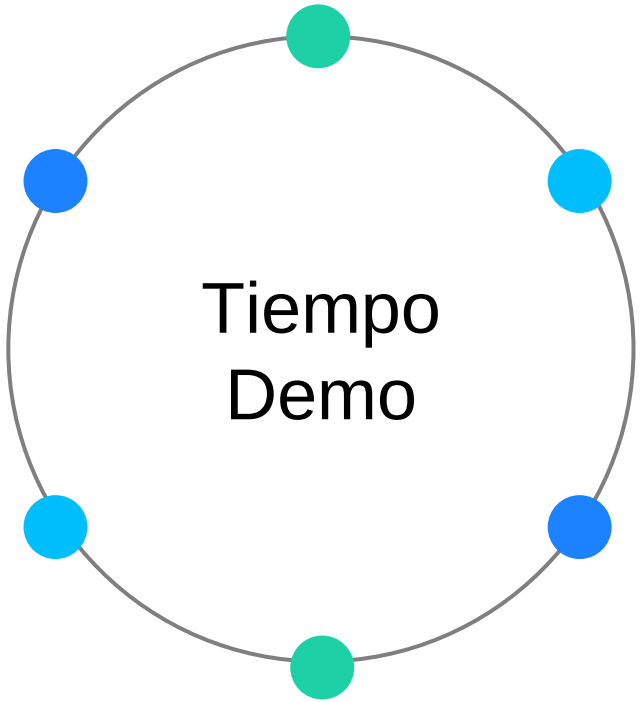
call apoc.meta.graph

Mapa gráfico de BBDD de NEO4J



Orquestación de Herramientas relacionando datos

GINSEG



Cruzcampo juntos…

Comunidad de inteligencia: https://ginseg.com
Grupo de Telegram: https://t.me/ginseg
Twitter: @gIntelSeg

GINSEG
Inteligencia y ciberseguridad

OSINT CITY

Crezcamos juntos…

Comunidad de inteligencia: https://ginseg.com
Grupo de Telegram: https://t.me/ginseg
Twitter: @gIntelSeg

GINSEG
Inteligencia y ciberseguridad

OSINT CITY