TLP:GREEN

RNEP-GW

MÓDULO INTELMQ

fct csirt

RNEP-GW

INTELMQ

Solução para equipas CSIRT e SOC

Agrupa e processa informação proveniente de diversas fontes de segurança

Enriquecimento e normalização da informação

Mecanismo de gestão de filas para processar volumes de informação gigantescos

intelmq.readthedocs.io

INTELMQ

Recolha automática de eventos

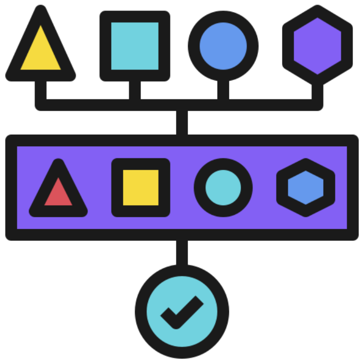
Harmonização de dados

Tipificação e classificação

Único formato – JSON

Facilitar a partilha da informação

Criação de blacklists



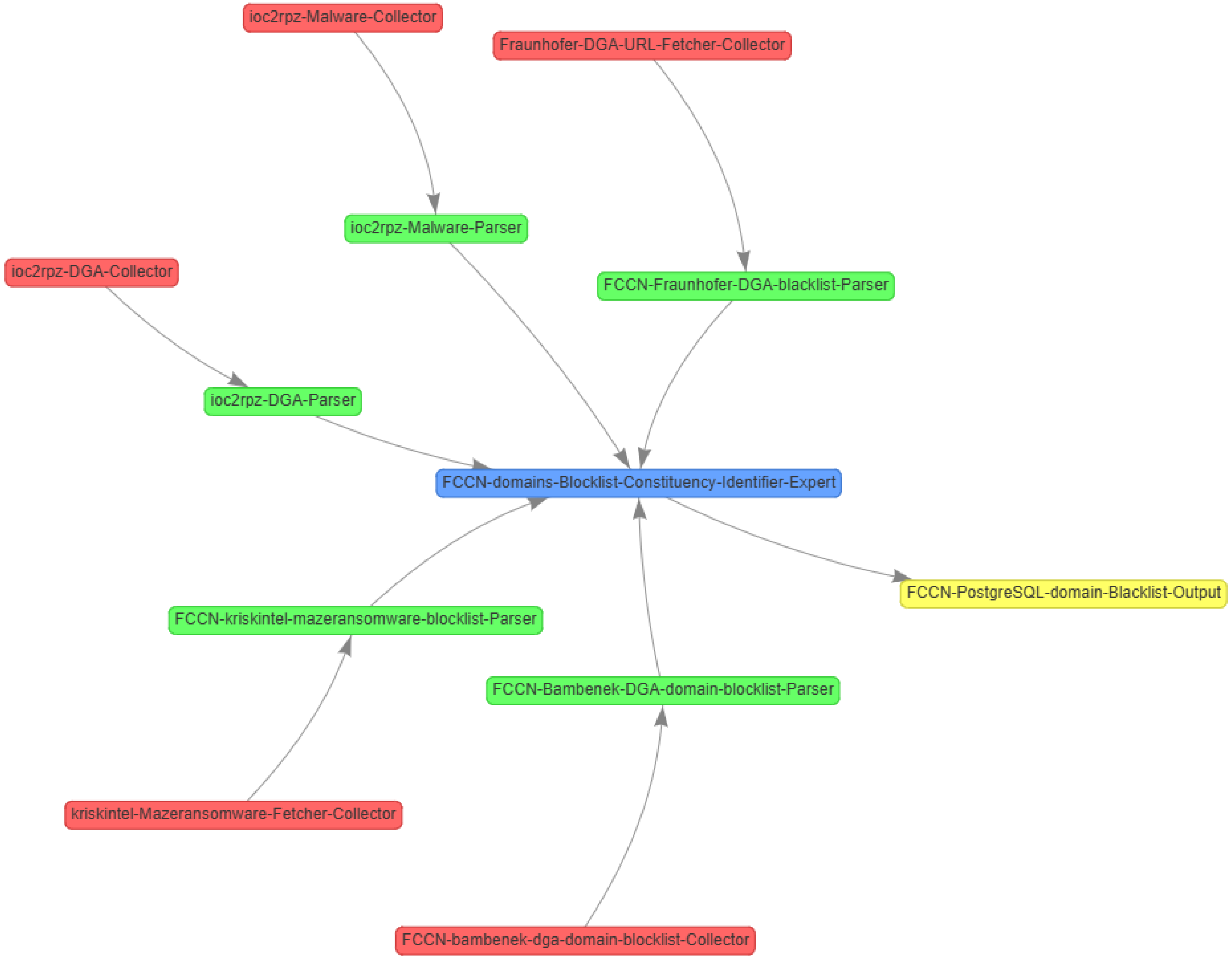
BOTS

Collectors

Parsers

Experts

Outputs



ioc2rpz-Malware-Collector

Fraunhofer-DGA-URL-Fetcher-Collector

ioc2rpz-Malware-Parser

ioc2rpz-DGA-Collector

FCCN-Fraunhofer-DGA-blacklist-Parser

ioc2rpz-DGA-Parser

FCCN-domains-Blocklist-Constituency-Identifier-Expert

FCCN-PostgreSQL-domain-Blacklist-Output

FCCN-kriskintel-mazeransomware-blocklist-Parser

FCCN-Bambenek-DGA-domain-blocklist-Parser

kriskintel-Mazeransomware-Fetcher-Collector

FCCN-bambenek-dga-domain-blocklist-Collector

COLLECTORS

AMQP

API

Files

Mail Attachment Fetcher

Mail URL fetcher

Mail Body Fetcher

URL Fetcher

URL stream Fetcher

Request Tracker

TCP

FTP

GitHub API

...

PARSERS

Abuse.ch

Openphish

Phishtank

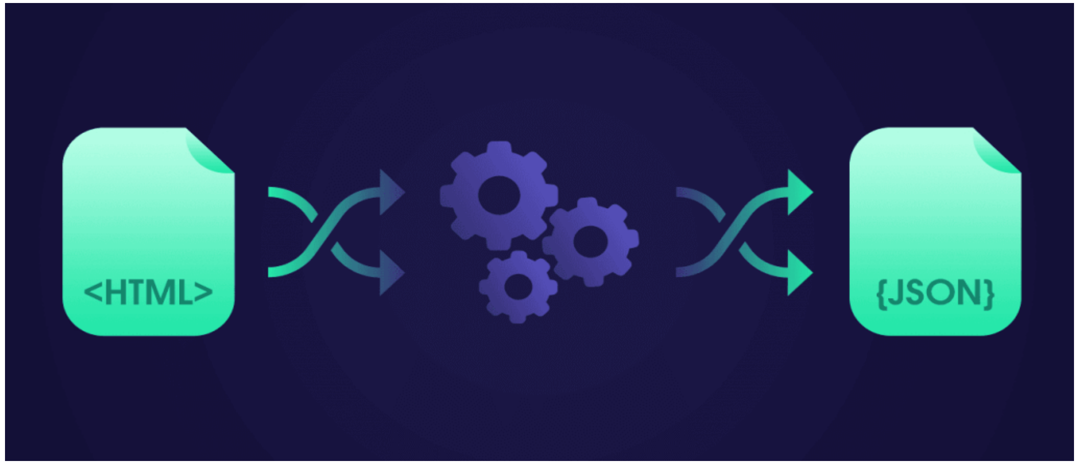
Spamhaus CERT

MISP

AlienVault

Cymru

Blocklist.de



EXPERTS

Deduplicator

ASN Loopup

Cymru Whois

Gethostbyname

Maxmind GeoIP

Reverse DNS

Taxonomy

Filters

OUTPUTS

Ficheiros

TCP/UDP

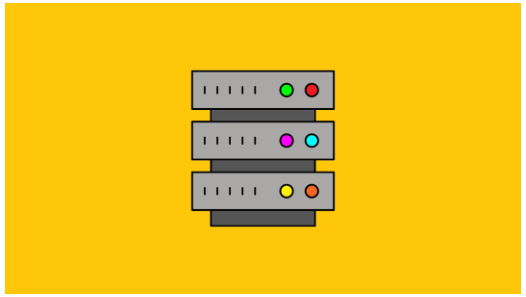
Email

Blackhole

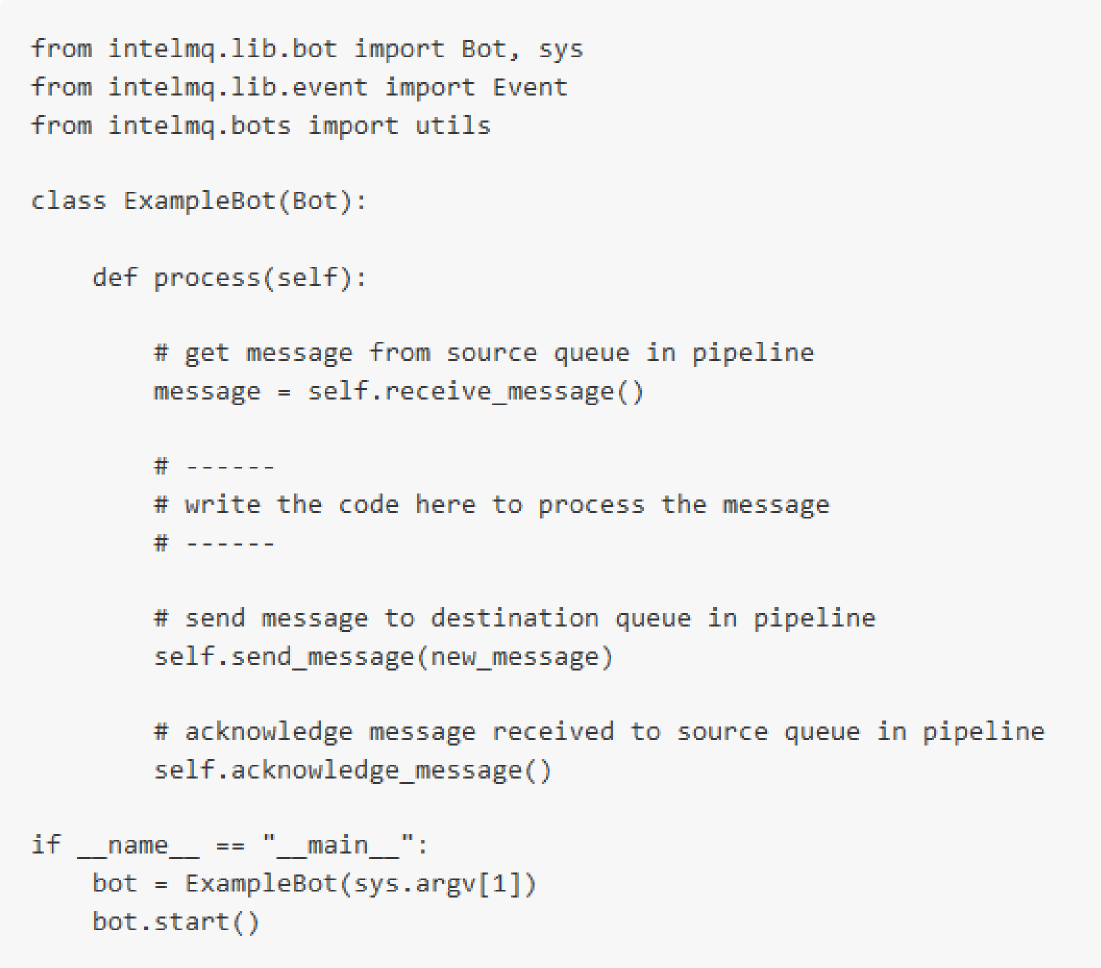
Bases de dados

- MongoDB
- ElasticSearch
- Redis
- Postgres
- Mysql
- Splunk

Event Writer



EXEMPLO DE UM BOT



```
from intelmq.lib.bot import Bot, sys
from intelmq.lib.event import Event
from intelmq.bots import utils

class ExampleBot(Bot):

    def process(self):

        # get message from source queue in pipeline
        message = self.receive_message()

        # ------
        # write the code here to process the message
        # ------

        # send message to destination queue in pipeline
        self.send_message(new_message)

        # acknowledge message received to source queue in pipeline
        self.acknowledge_message()

if __name__ == "__main__":
    bot = ExampleBot(sys.argv[1])
    bot.start()
```

CLI

Iniciar um bot:

```
intelmqctl start bot-id
```

Parar um bot:

```
intelmqctl stop bot-id
```

Reler as configs de um bot:

```
intelmqctl reload bot-id
```

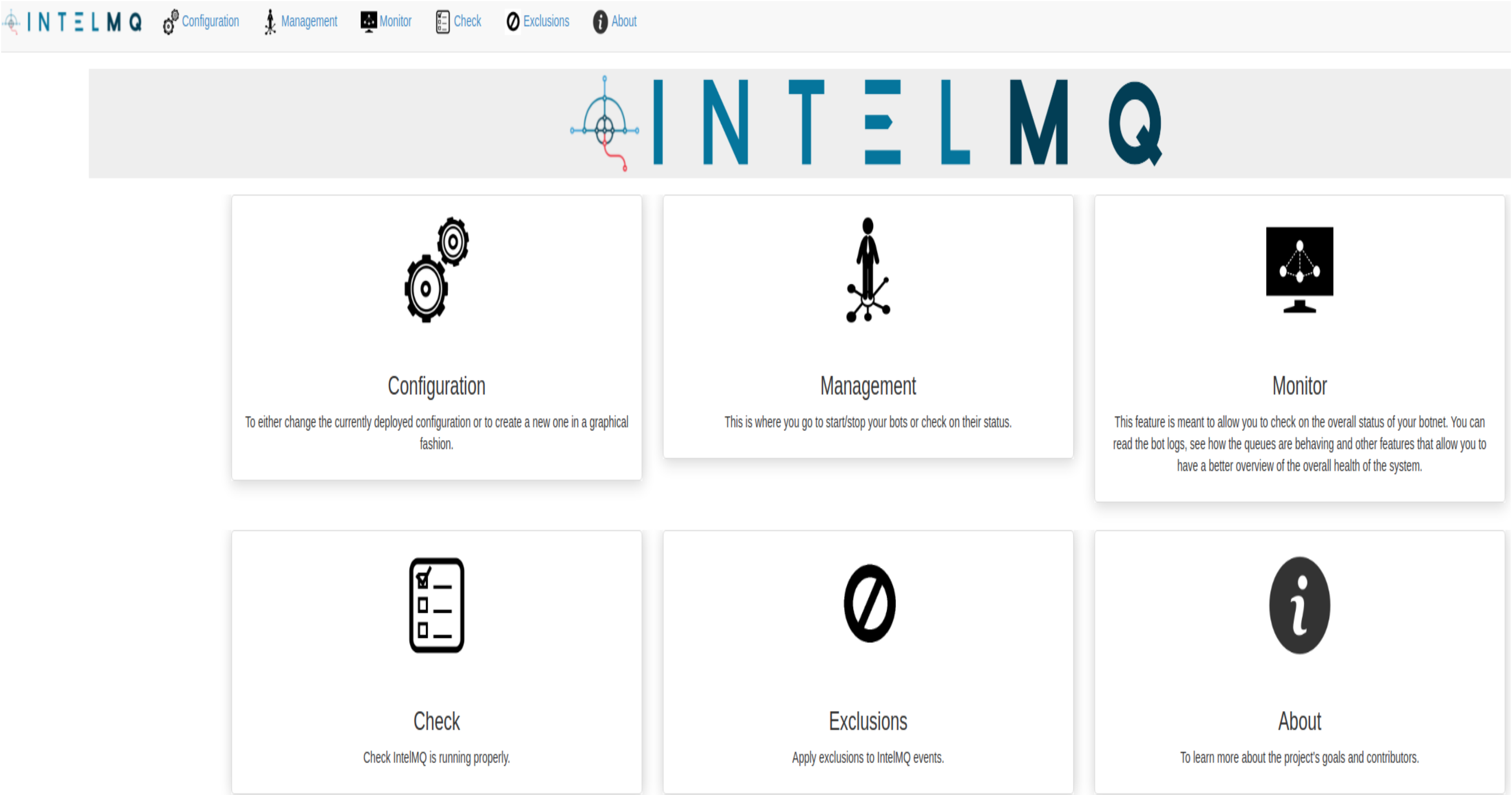
Reiniciar um bot:

```
intelmqctl restart bot-id
```

Iniciar todos os bots (botnet):

```
intelmqctl start
```

GRAPHICAL USER INTERFACE



Configuration

To either change the currently deployed configuration or to create a new one in a graphical fashion.

Management

This is where you go to start/stop your bots or check on their status.

Monitor

This feature is meant to allow you to check on the overall status of your botnet. You can read the bot logs, see how the queues are behaving and other features that allow you to have a better overview of the overall health of the system.

Check

Check IntelMQ is running properly.

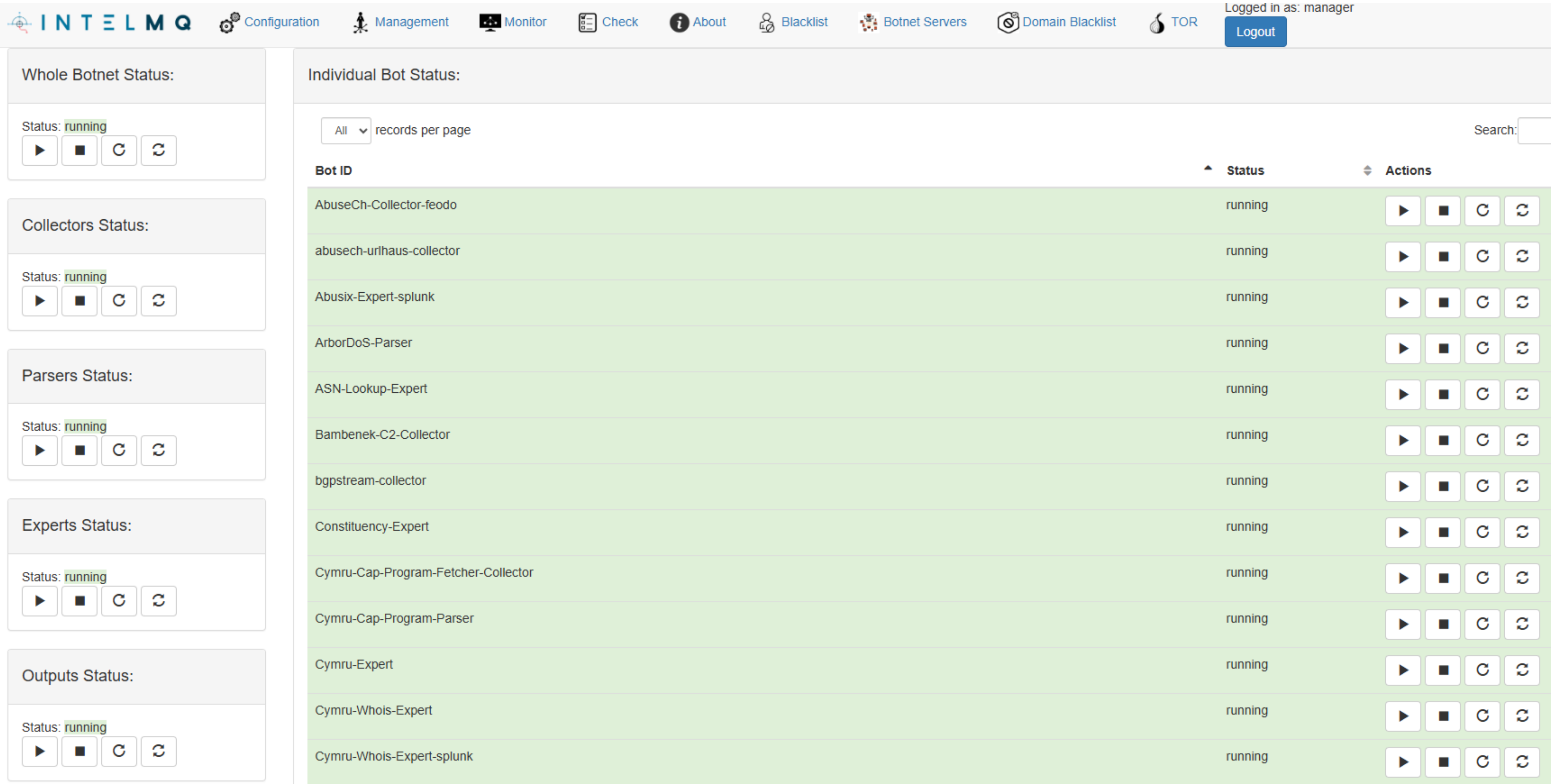
Exclusions

Apply exclusions to IntelMQ events.

About

To learn more about the project's goals and contributors.

CONSOLA DE GESTÃO



Whole Botnet Status:

Status: running

▶ ■ ↻ ⟳

Collectors Status:

Status: running

▶ ■ ↻ ⟳

Parsers Status:

Status: running

▶ ■ ↻ ⟳

Experts Status:

Status: running

▶ ■ ↻ ⟳

Outputs Status:

Status: running

▶ ■ ↻ ⟳

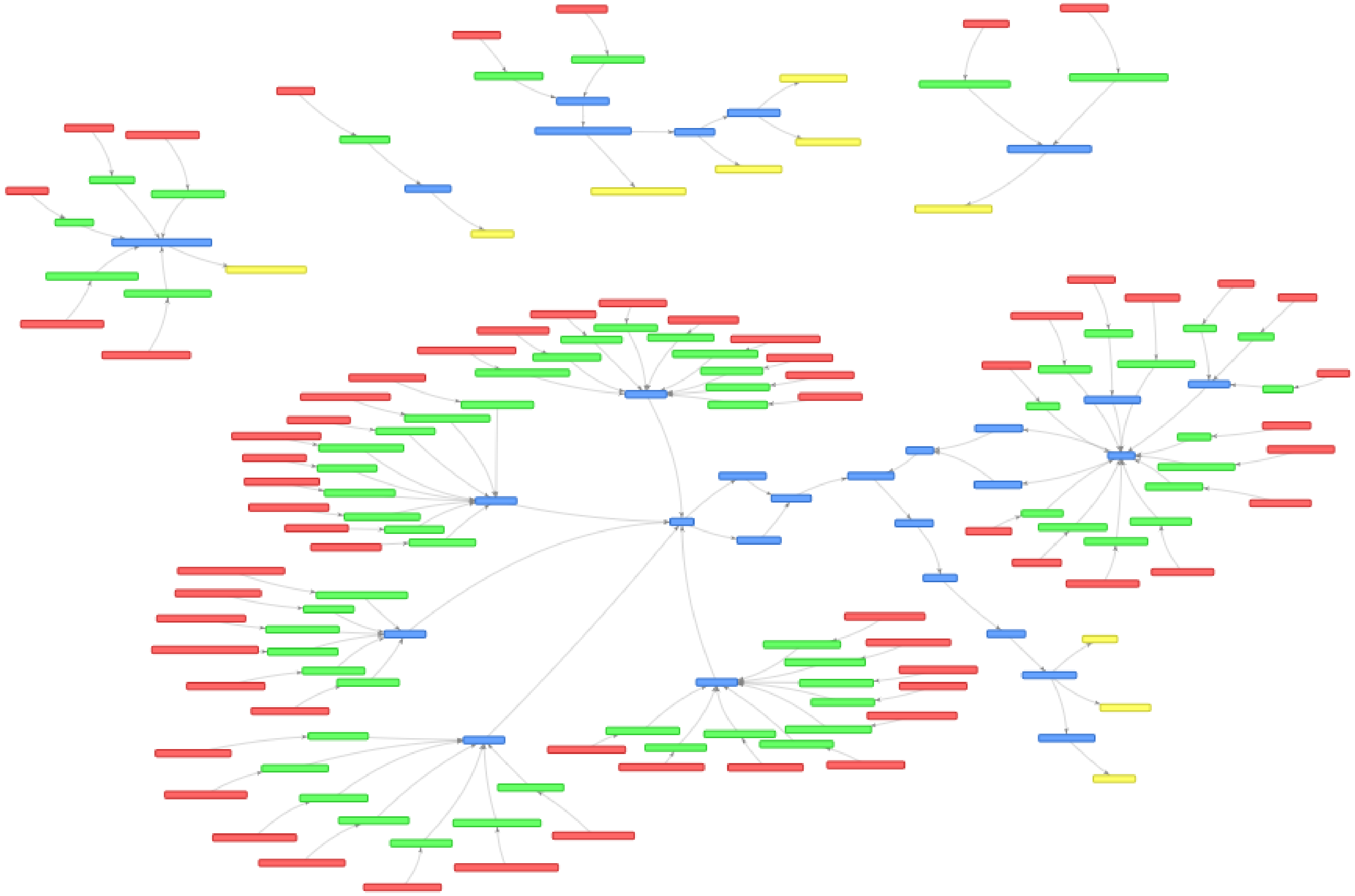
Individual Bot Status:

All records per page

Search:

Bot ID	Status	Actions
AbuseCh-Collector-feodo	running	▶ ■ ↻ ⟳
abusech-urlhaus-collector	running	▶ ■ ↻ ⟳
Abusix-Expert-splunk	running	▶ ■ ↻ ⟳
ArborDoS-Parser	running	▶ ■ ↻ ⟳
ASN-Lookup-Expert	running	▶ ■ ↻ ⟳
Bambenek-C2-Collector	running	▶ ■ ↻ ⟳
bgpstream-collector	running	▶ ■ ↻ ⟳
Constituency-Expert	running	▶ ■ ↻ ⟳
Cymru-Cap-Program-Fetcher-Collector	running	▶ ■ ↻ ⟳
Cymru-Cap-Program-Parser	running	▶ ■ ↻ ⟳
Cymru-Expert	running	▶ ■ ↻ ⟳
Cymru-Whois-Expert	running	▶ ■ ↻ ⟳
Cymru-Whois-Expert-splunk	running	▶ ■ ↻ ⟳

MAPA DE BOTS



ESTRUTURA

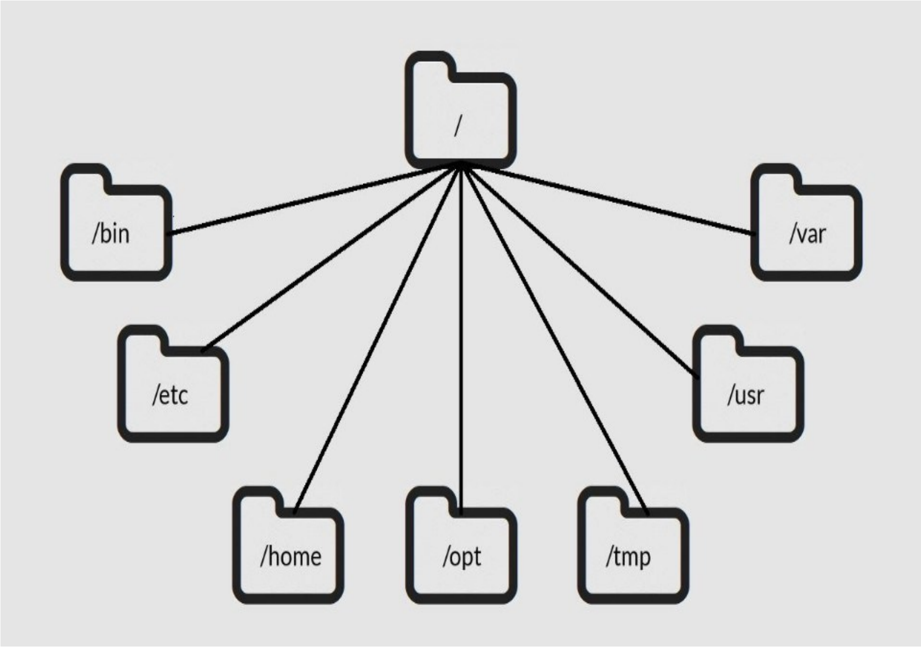
/etc/intelmq

/var/lib/intelmq

/var/lib/intelmq/bots

/var/log/intelmq

/var/run/intelmq



FICHEIROS IMPORTANTES

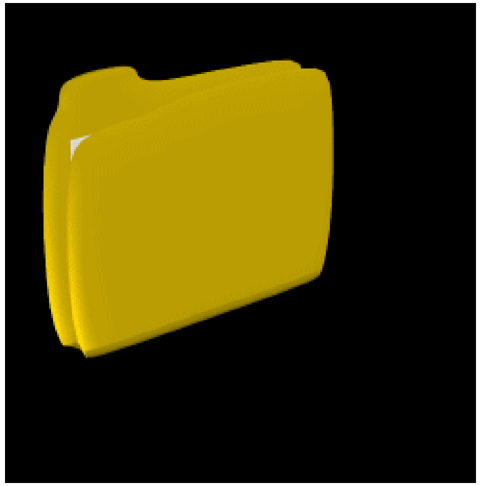
defaults.conf

system.conf

startup.conf

runtime.conf

ipeline.conf



AVALIAÇÃO

Vantagens:

- WorkFlow de compreensão
- Bots existentes
- Loosely de-coupled
- Open-source code

Desvantagens:

- Python
- Upstream
- Ticket systems
- Data loss

IDEIAS CHAVE

- O IntelMQ é uma solução grátis para realizar o tratamento de inteligência de ameaças
- A ferramenta assenta em código python
- Existem bots “pré-feitos”, o que facilita a adopção da ferramenta

Questões?

Obrigado.

PODCAST
CERT RCTS
DIZ-ME A TUA PASSWORD, DIR-TE-EI QUEM ÉS
\\:podcast\segurança-informática
fct Fundação para a Ciência e a Tecnologia
FCCN

csirt.fct.pt/podcast

Exact Sciences and Technology
CSIRT in a Box: Capacitação Inicial de Equipas de Resposta a Incidentes
nau SEMPRE A APRENDER by FCCN fct

csirt.fct.pt/mooc

csirt.fct.pt/etc