

# INTELMQ

Pedro Silva



# Agenda

- Introdução
- Arquitectura
- Interacção
- Vantagens vs Desvantagens



# INTRODUÇÃO



# O que é o IntelMQ?

*«IntelMQ is a solution to process data feeds, pastebins, tweets through a message queue.»*

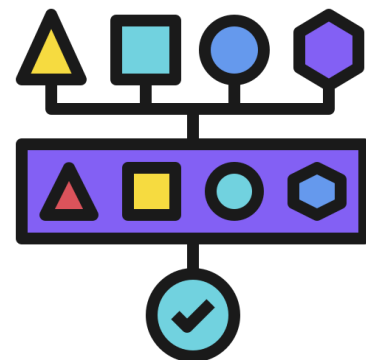
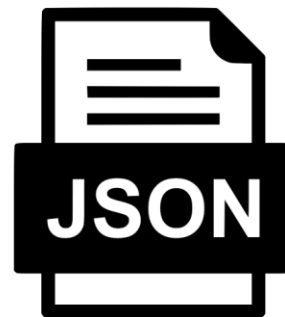
(ex-)CERT.PT

CERT.AT



# Funcionalidades do IntelMQ

- Recolha automática de eventos
- Harmonização de dados
- Tipificação e classificação
- Único formato – JSON
- Facilitar a partilha da informação
- Criação de blacklists

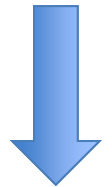
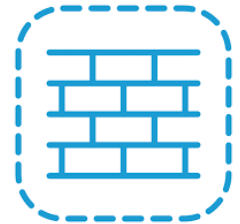


# ARQUITECTURA



# Bots

**Collector 1**



**Parser 1**

**Protocol  
Expert**

**Event Writer**

- Collectors
- Parsers
- Experts
- Outputs

# 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()
```





# 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
- ...

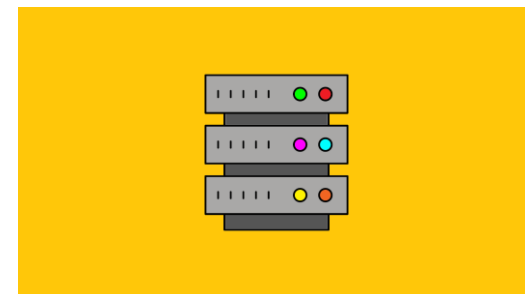


# Outputs

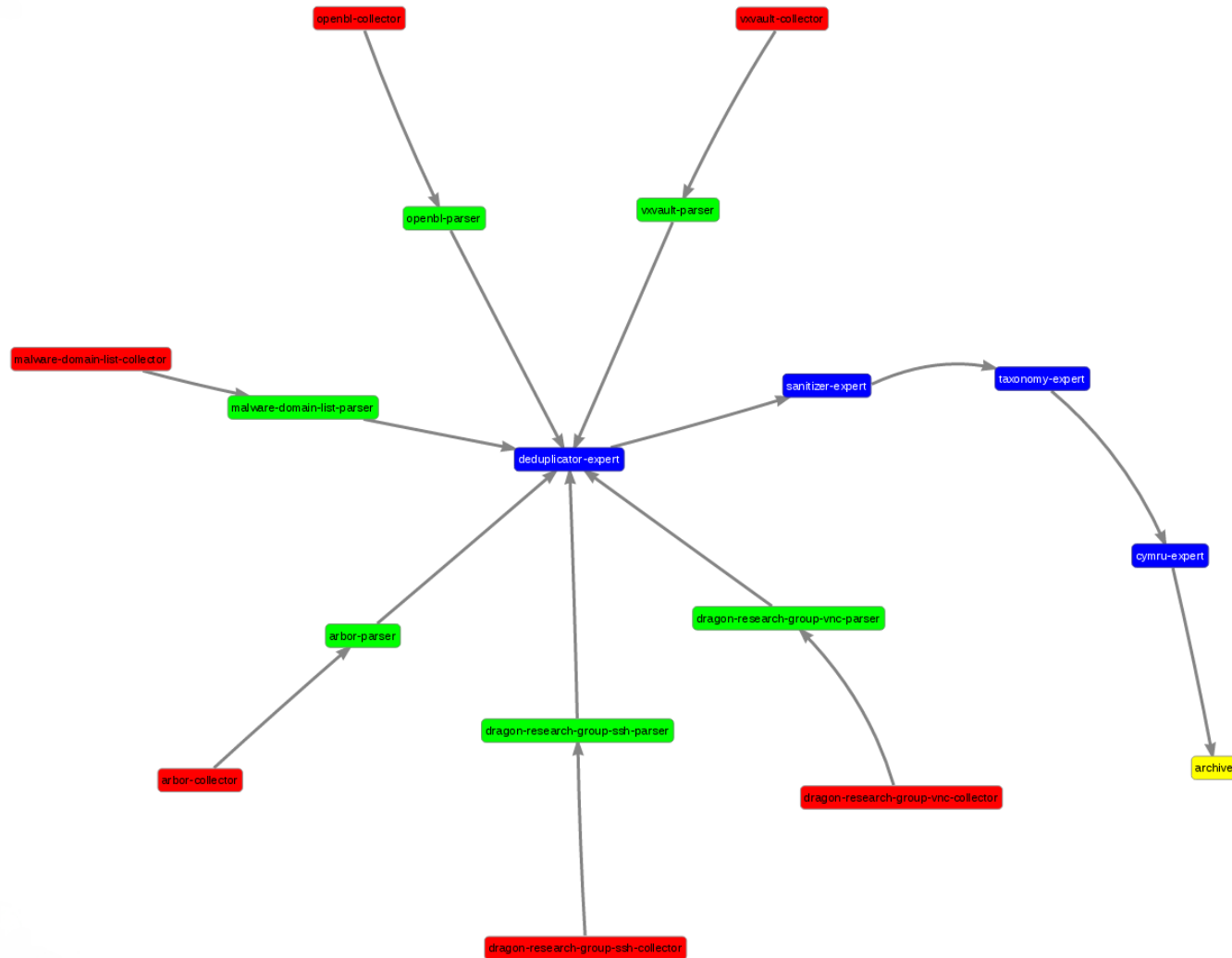
- Ficheiros
- TCP/UDP
- Bases de dados
  - MongoDB
  - ElasticSearch
  - Redis
  - Postgres
  - Mysql
  - Splunk
  - ...
- Email
- BlackHole
- ...



**Event Writer**



# Esquema da ligação entre bots



# INTERACÇÃO



# 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**
- See additional help for further explanation.  
**intelmqctl run bot-id --help**
- 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.

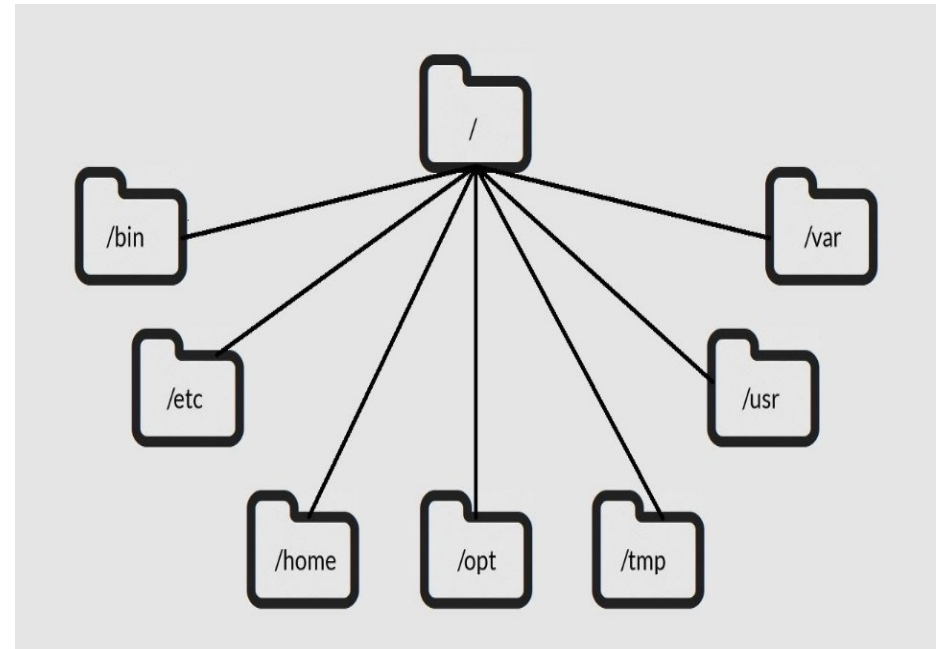


## About

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

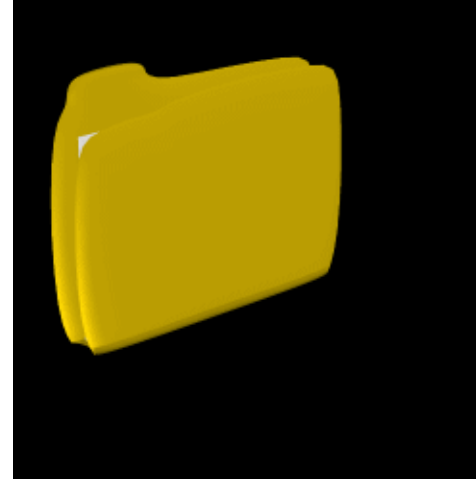
# Estrutura de directorias

- `/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



# VANTAGENS vs DESVANTAGENS

- **Vantagens:**

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




- **Desvantagens:**

- Python
- Upstream
- Ticket systems
- Data loss





# Em Resumo

-  Recolha automática e harmonização de eventos
-  Um lugar único e central de gestão
-  Conhecimentos em Python



# Obrigado