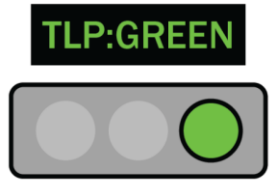


RNEP-GW

MÓDULO AUTOMAÇÃO

fct csirt

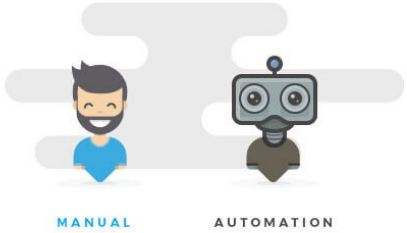
RNEP-GW

CI/CD

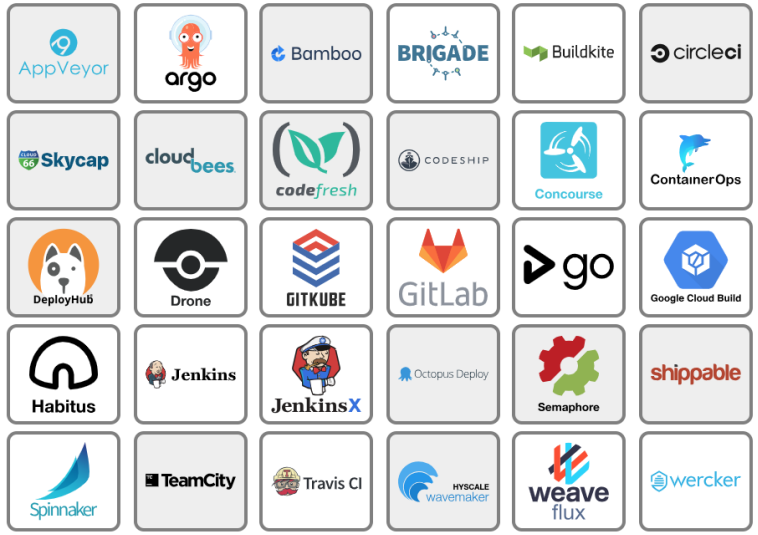
CI / CD

O que é CI/CD?

Porque deve ser usada?



Que software usar?



JENKINS

Uma vasta comunidade com muita documentação

Fácil utilização

Web GUI

Um project maduro (2004 Hudson)

Plugins (JIRA, UIs, Authentication, GitLab etc.)

Usado por grandes organizações:

GitHub

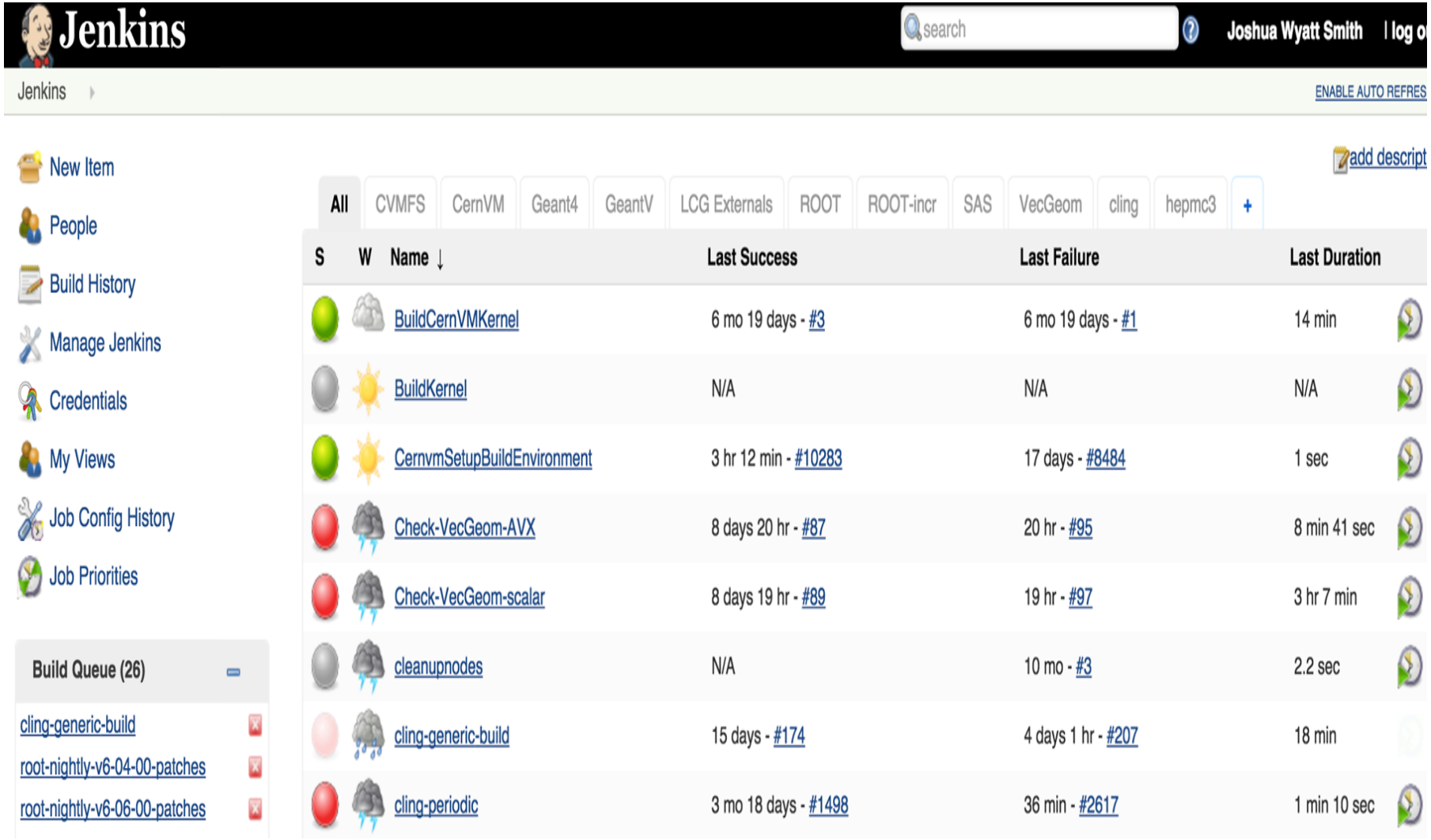
CERN

DELL

ebay

LinkedIn

JENKINS - GUI

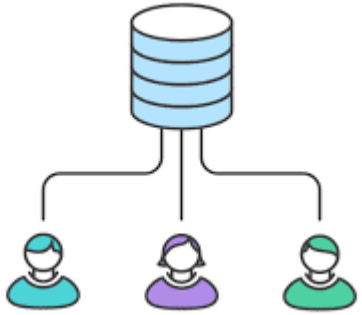

Jenkins
search
Joshua Wyatt Smith
Jenkins
ENABLE AUTO REFRES
New Item
People
Build History
Manage Jenkins
Credentials
My Views
Job Config History
Job Priorities
add descript
All
CVMFS
CernVM
Geant4
GeantV
LCG Externals
ROOT
ROOT-incr
SAS
VecGeom
cling
hepmc3
+
S
W
Name ↓
Last Success
Last Failure
Last Duration
BuildCernVMKernel
6 mo 19 days - #3
6 mo 19 days - #1
14 min
BuildKernel
N/A
N/A
N/A
CernvmSetupBuildEnvironment
3 hr 12 min - #10283
17 days - #8484
1 sec
Check-VecGeom-AVX
8 days 20 hr - #87
20 hr - #95
8 min 41 sec
Check-VecGeom-scalar
8 days 19 hr - #89
19 hr - #97
3 hr 7 min
cleanupnodes
N/A
10 mo - #3
2.2 sec
cling-generic-build
15 days - #174
4 days 1 hr - #207
18 min
cling-periodic
3 mo 18 days - #1498
36 min - #2617
1 min 10 sec
Build Queue (26)
cling-generic-build
root-nightly-v6-04-00-patches
root-nightly-v6-06-00-patches

REPOSITÓRIO

REPOSITÓRIO

O que é um repositório?

Porque deve ser usado?



Que software usar?

Bit Bucket

GitHub

GitLab

GITLAB

- Gratuito
- Opensource
- Web GUI
- Privados/Publicos
- Grupos
- REST API
- Versionamento
- Integração com CI/CD

AUTOMAÇÃO DE PROCESSOS: ANSIBLE

AUTOMATIZAÇÃO

Porque deve ser usado?

Que software usar?

puppet labs

CHEF

SALTSTACK

ANSIBLE

MANUAL

```
root@server:~# # Install the PGP key
root@server:~# gpg --keyserver keyserver.ubuntu.com --recv-keys 561F9B9CAC40B
root@server:~# gpg --armor --export 561F9B9CAC40B2F7 | sudo apt-key add -

root@server:~# # Install https support for apt
root@server:~# apt-get install apt-transport-https

root@server:~# # Add the passenger apt repository
root@server:~# vi /etc/apt/sources.list.d/passenger.list
root@server:~# chown root: /etc/apt/sources.list.d/passenger.list
root@server:~# chmod 600 /etc/apt/sources.list.d/passenger.list

root@server:~# # Update the apt cache so we can use the new repo
root@server:~# apt-get update

root@server:~# # Install nginx
root@server:~# apt-get install nginx-full passenger

root@server:~# # Set up passenger in the nginx configuration
root@server:~# vi /etc/nginx/nginx.conf

root@server:~# # Start nginx
root@server:~# service nginx restart
```

SHELL SCRIPT

```
# Install the PGP key
gpg --keyserver keyserver.ubuntu.com --recv-keys 561F9B9CAC40B2F7
gpg --armor --export 561F9B9CAC40B2F7 | apt-key add -

# Install https support for apt
apt-get install apt-transport-https -y

# Add the passenger apt repository
echo "deb https://oss-binaries.phusionpassenger.com/apt/passenger raring main"
chown root: /etc/apt/sources.list.d/passenger.list
chmod 600 /etc/apt/sources.list.d/passenger.list

# Update the apt cache so we can use the new repo
apt-get update

# Install nginx
apt-get install nginx-full passenger -y

# Set up passenger in the nginx configuration
sed -i "s/# passenger_root/passenger_root/" /etc/nginx/nginx.conf
sed -i "s/# passenger_ruby/passenger_ruby/" /etc/nginx/nginx.conf

# Start nginx
service nginx restart
```

ANSIBLE

```
---
- hosts: all
  tasks:

  - name: Ensure the PGP key is installed
    apt_key: >
      state=present
      id=AC40B2F7
      url="http://keyserver.ubuntu.com/pks/lookup?op=get&fingerprint=on&search

  - name: Ensure https support for apt is installed
    apt: >
      state=present
      pkg=apt-transport-https

  - name: Ensure the passenger apt repository is added
    apt_repository: >
      state=present
      repo='deb https://oss-binaries.phusionpassenger.com/apt/passenger raring

  - name: Ensure nginx is installed
    apt: >
      state=present
      pkg=nginx-full

  - name: Ensure passenger is installed
    apt: >
      state=present
      pkg=passenger
      update_cache=yes

  - name: Ensure the nginx configuration file is set
    copy: >
      src=/app/config/nginx.conf
      dest=/etc/nginx/nginx.conf

  - name: Ensure nginx is running
    service: >
      name=nginx
      state=started
```

CASOS PRÁTICOS

Criar utilizadores

Patches de Segurança

Gestão de regras de FW

Distribuição e rotatividade:

- Chaves SSH (Mais Seguro)
- Passwords (Menos Seguro)

Inventário

- Qual o software usado no parque informático?
- Em que servidores está instalado?

CASOS PRÁTICOS

Auditorias

- O ficheiro 123.txt existe nos nossos servidores? Quais?
- O utilizador color existe nos nossos servidores? Quais?

Fazer tarefas repetitivas:

- Reboot de máquinas
- Cronjobs
- Deployment de Software

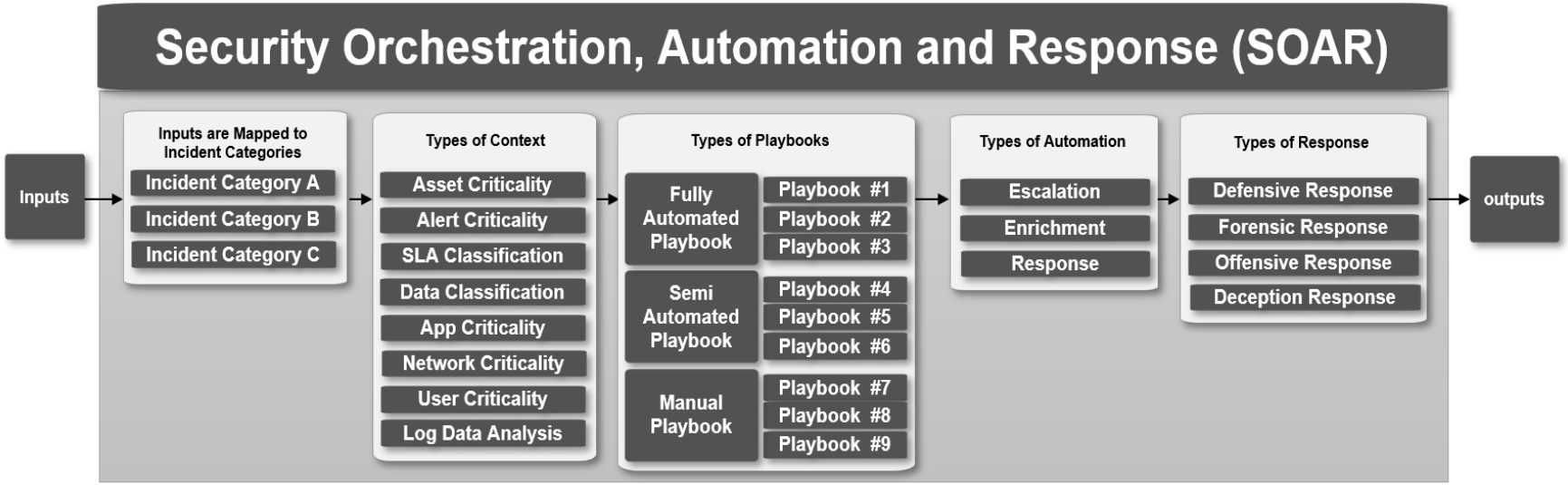
Upgrades:

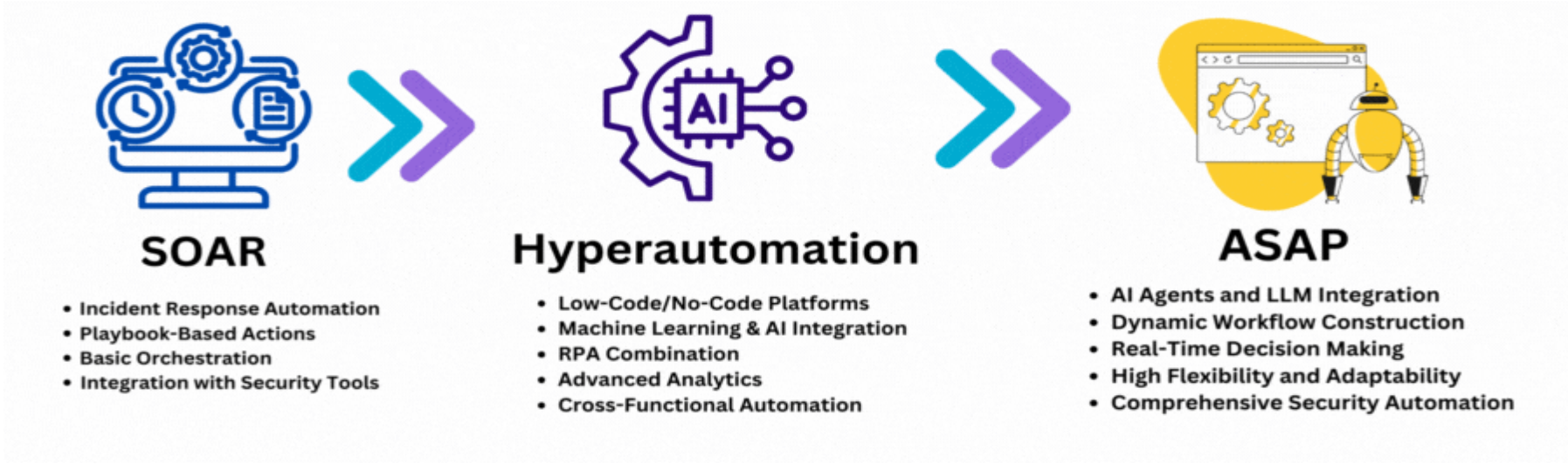
- Software
- OSs

AUTOMAÇÃO EM CYBER SEGURANÇA

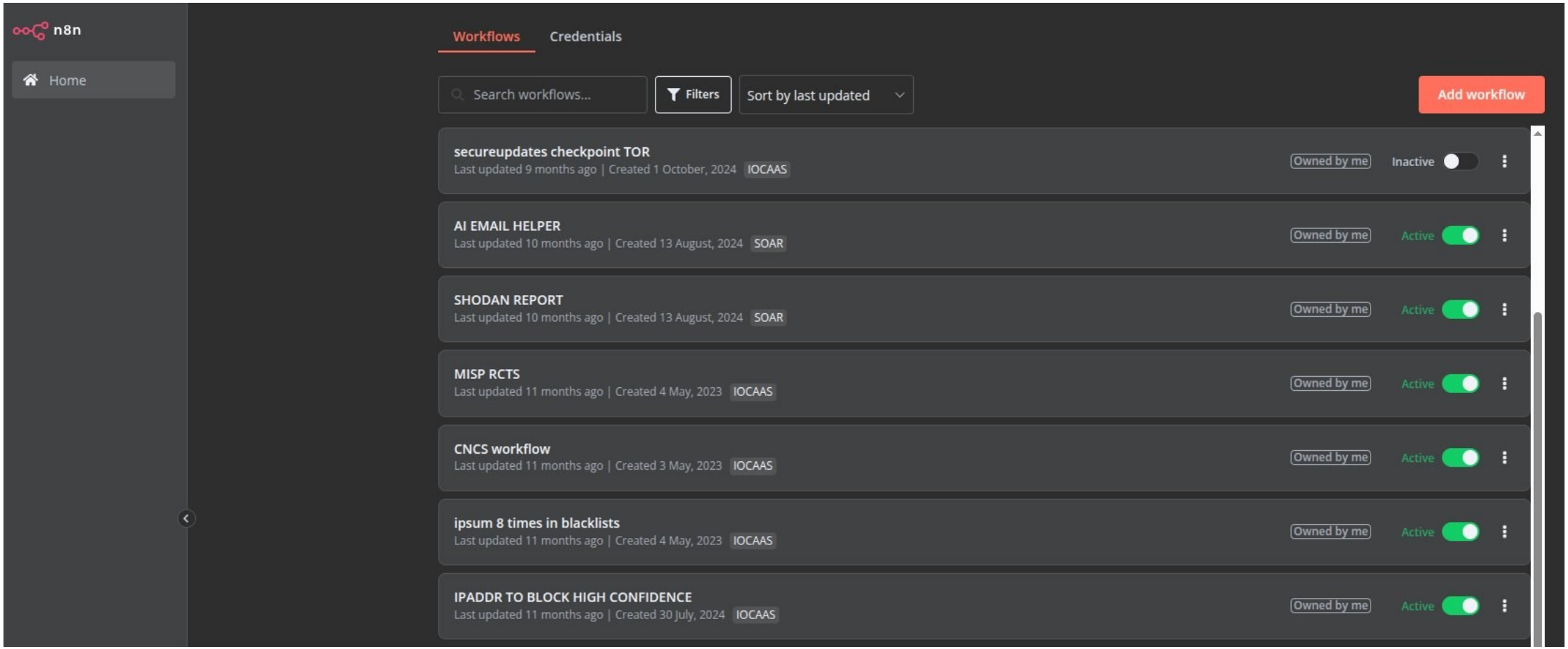
SECURITY ORCHESTRATION, AUTOMATION AND RESPONSE

SECURITY ORCHESTRATION, AUTOMATION AND RESPONSE

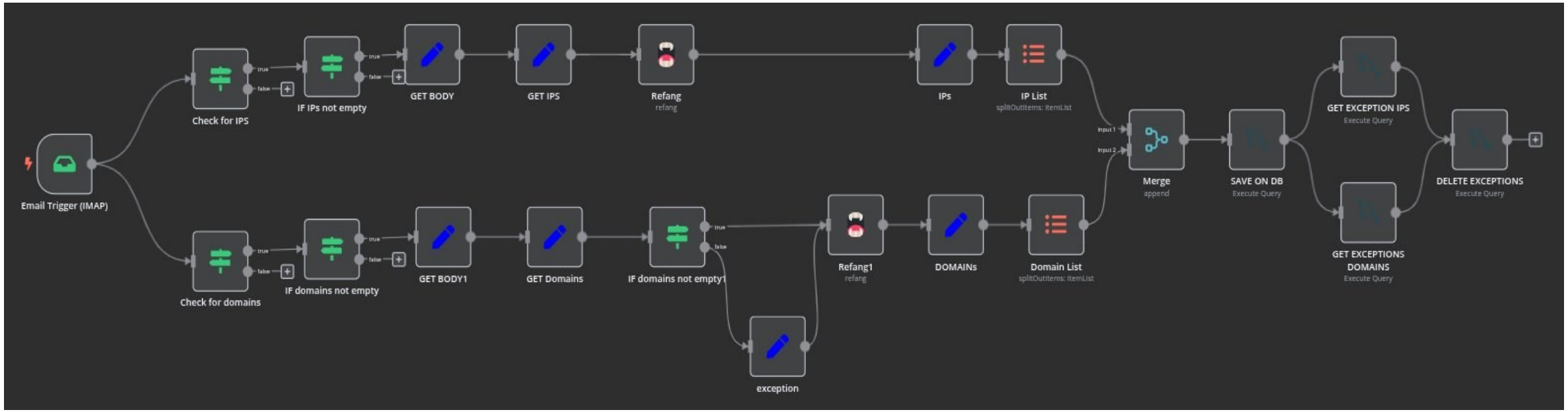




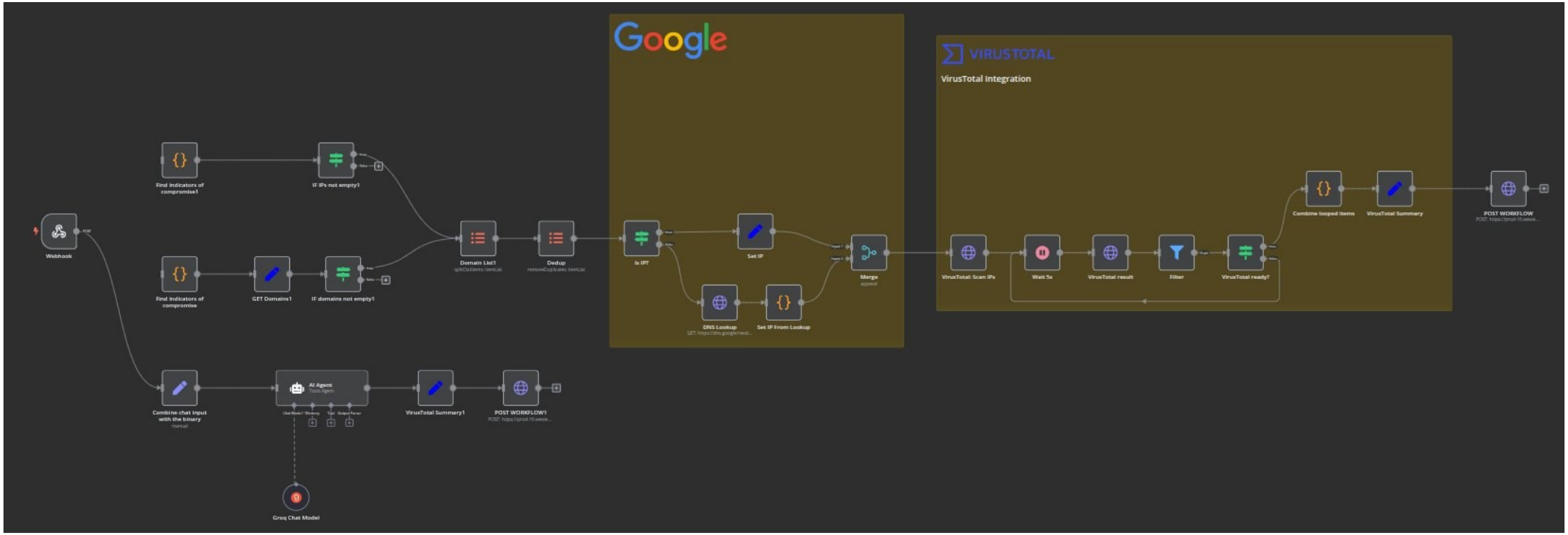
N8N


n8n
Home
Workflows
Credentials
Search workflows...
Filters
Sort by last updated
Add workflow
secureupdates checkpoint TOR
Last updated 9 months ago | Created 1 October, 2024 IOCAAS
Owned by me
Inactive
AI EMAIL HELPER
Last updated 10 months ago | Created 13 August, 2024 SOAR
Owned by me
Active
SHODAN REPORT
Last updated 10 months ago | Created 13 August, 2024 SOAR
Owned by me
Active
MISP RCTS
Last updated 11 months ago | Created 4 May, 2023 IOCAAS
Owned by me
Active
CNCS workflow
Last updated 11 months ago | Created 3 May, 2023 IOCAAS
Owned by me
Active
ipsum 8 times in blacklists
Last updated 11 months ago | Created 4 May, 2023 IOCAAS
Owned by me
Active
IPADDR TO BLOCK HIGH CONFIDENCE
Last updated 11 months ago | Created 30 July, 2024 IOCAAS
Owned by me
Active

N8N


Email Trigger (IMAP)
Check for IPS
IF IPs not empty
GET BODY
GET IPS
Refang
refang
IPs
IP List
splitOutItems: ItemList
Check for domains
IF domains not empty
GET BODY1
GET Domains
IF domains not empty1
exception
Refang1
refang
DOMAINs
Domain List
splitOutItems: ItemList
Merge
append
SAVE ON DB
Execute Query
GET EXCEPTION IPS
Execute Query
GET EXCEPTIONS DOMAINS
Execute Query
DELETE EXCEPTIONS
Execute Query

N8N


Google
VIRUSTOTAL
VirusTotal Integration
Webhook
Find indicators of compromise1
IF IPs not empty1
Find indicators of compromise
GET Domains1
IF domains not empty1
Domain List1
Dedup
Is IP?
Set IP
DNS Lookup
Set IP From Lookup
Merge
VirusTotal: Scan IPs
Wait 5s
VirusTotal result
Filter
VirusTotal ready?
Combine looped items
VirusTotal Summary
POST WORKFLOW
Combine chat input with the binary
AI Agent
VirusTotal Summary1
POST WORKFLOW1
Groq Chat Model

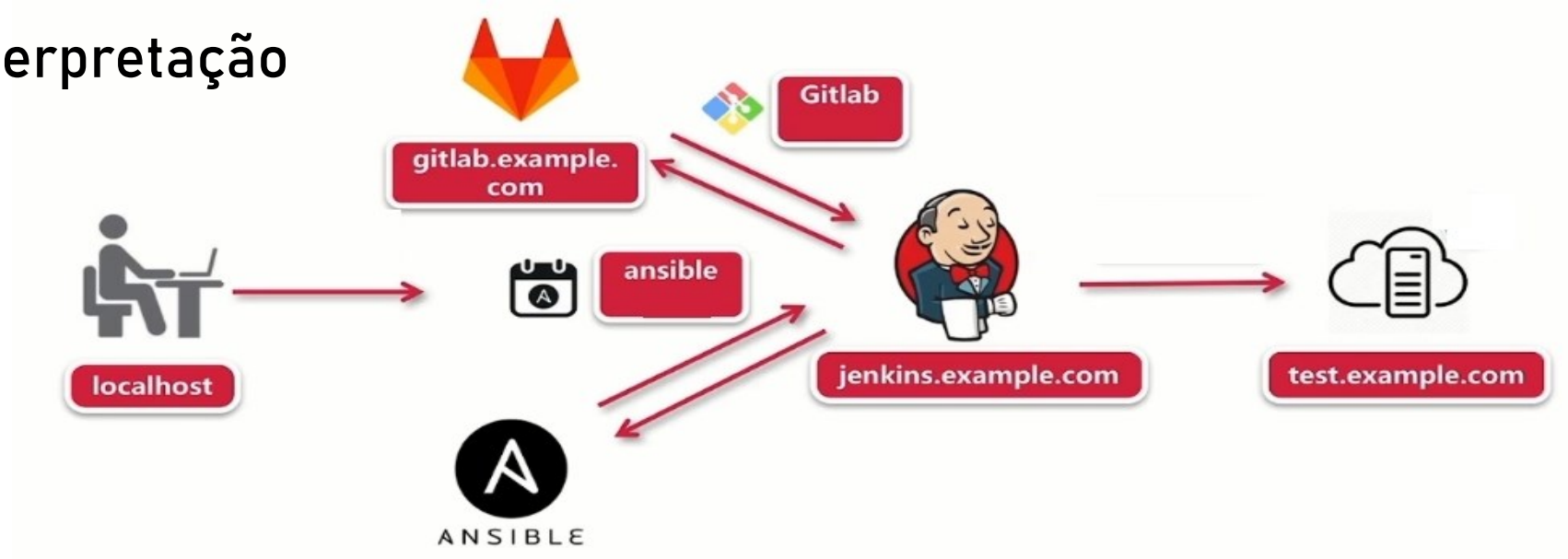
VANTAGENS VS DESVANTAGENS

VANTAGENS

- Simples e conciso
- Redução do tempo
- Estruturado
- Fácil leitura / interpretação
- Colaboração

DESVANTAGENS

- Aprender um novo paradigma
- Alterar o processo existente



EM RESUMO

- Aumentar a Produtividade
- Aumentar a segurança
- Ampla gama de ferramentas open-source disponíveis

Questões?

Obrigado.

csirt.fct.pt/podcast

csirt.fct.pt/mooc

csirt.fct.pt/etc