BRASIL campus party

TALK – PALCO CODERS

CRIANDO UMA INTELIGÊNCIA ARTIFICIAL PARA SEGURANÇA DA INFORMAÇÃO

PEDRO BEZERRA

COGNITIVE SECURITY | INFORMATION SECURITY | GRC |+| RESEARCHER | LECTURE | COMMUNITY MANAGER OF AI AND SECURITY

No mundo real ...

Al que bate em Chico também bate em Francisco!

AI Brasil
an artificial intelligence community

Comunidades

Security H1V3

Meetup.com: https://www.meetup.com/pt-BR/Security-Hive/

Youtube: *Procurar por Security H1V3*

Grupos em Apps: Entre na nossa página do Meetup.com e fale com Pedro Bezerra.

AI Brasil

Meetup.com: https://www.meetup.com/pt-BR/ai-brasil

Youtube:https://www.youtube.com/c/AIBrasilCommunity

Grupos em Apps: Entre na nossa página do Meetup.com e fale com Pedro Bezerra.

Fonte (Google): Stranger Things - NetFlix

security H1VE

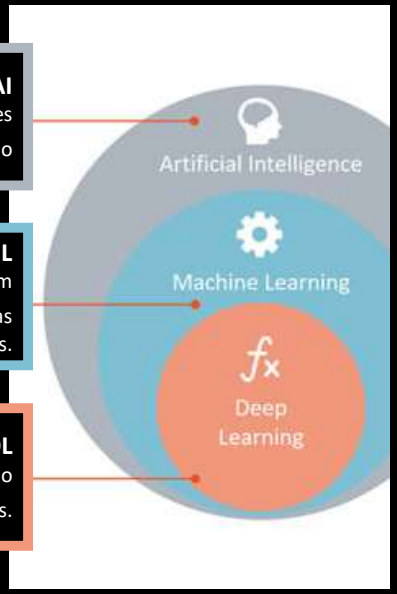
AI Brasil
an artificial intelligence community

AI, Machine Learning, Deep Learning e NLP

Artificial Intelligence - AI
Qualquer técnica que permita aos computadores **imitar** o comportamento humano

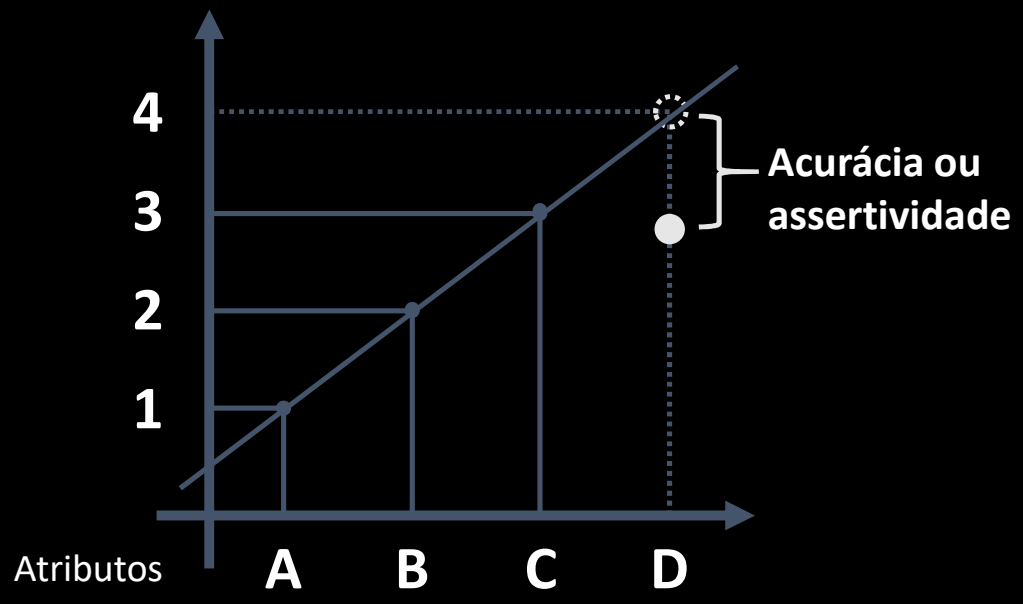
Machine Learning - ML
Subconjunto de técnicas de AI que utilizam **métodos estatísticos** para permitir que as máquinas melhorem com experiências.

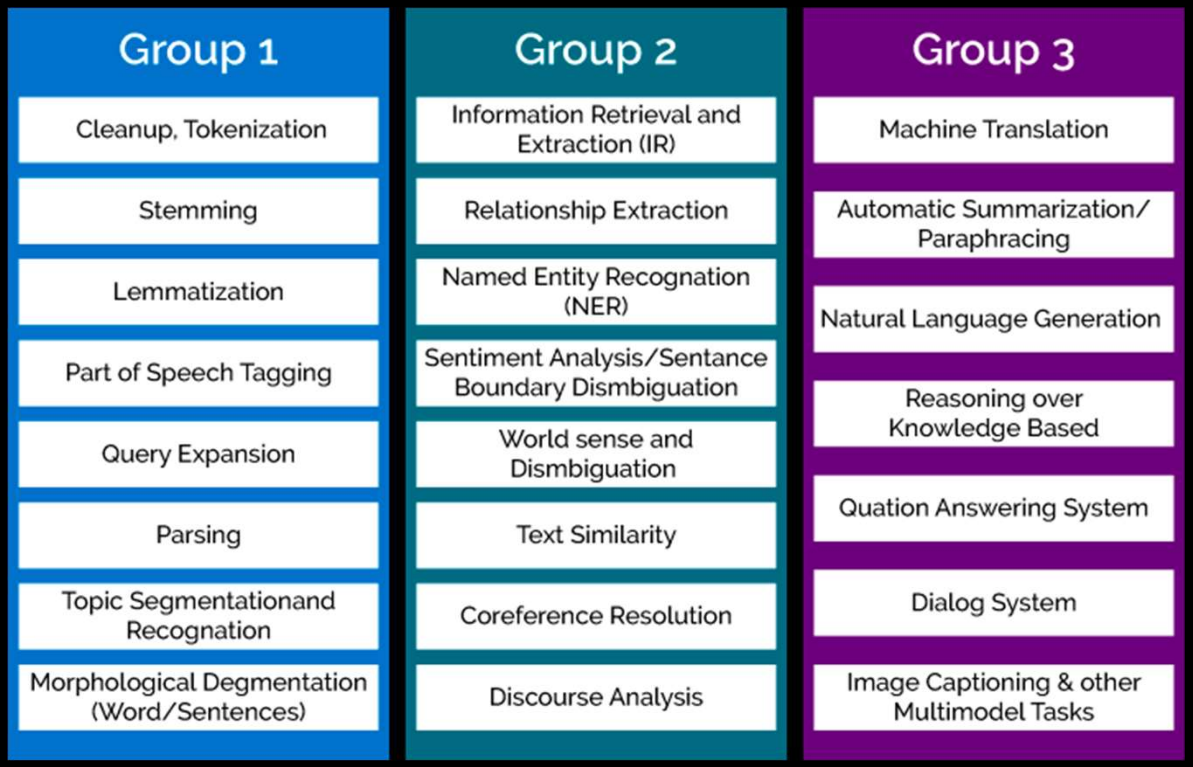
Deep Learning - DL
Subconjunto de ML que possibilita a computação de **redes neurais** de várias camadas.



Fontes:
https://content-static.upwork.com/blog/uploads/sites/3/2017/06/27091427/image-43.png
http://biogeocarlos.blogspot.com.br/2009/04/arte-zoologia-iv-camaleon.html

Tentando simplificar




Group 1
Cleanup, Tokenization
Stemming
Lemmatization
Part of Speech Tagging
Query Expansion
Parsing
Topic Segmentationand Recognation
Morphological Degmentation (Word/Sentences)
Group 2
Information Retrieval and Extraction (IR)
Relationship Extraction
Named Entity Recognation (NER)
Sentiment Analysis/Sentance Boundary Dismbiguation
World sense and Dismbiguation
Text Similarity
Coreference Resolution
Discourse Analysis
Group 3
Machine Translation
Automatic Summarization/ Paraphracing
Natural Language Generation
Reasoning over Knowledge Based
Quation Answering System
Dialog System
Image Captioning & other Multimodel Tasks

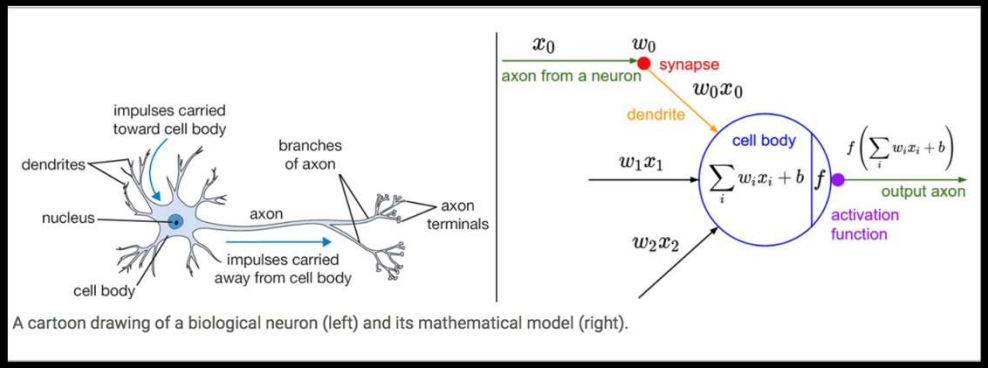

LET'S START SOME SHIT
COME ON.
memes.com

#CODANDO

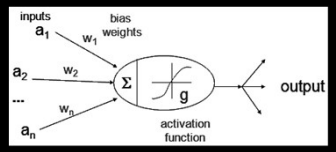
Usando a matemática para criar sua IA

Nível de complexidade, ou ... quanto trabalho isso dá !!

Neurónios humanos e *Perceptrons*



A cartoon drawing of a biological neuron (left) and its mathematical model (right).



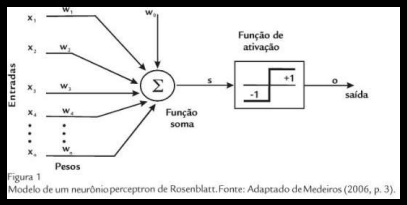
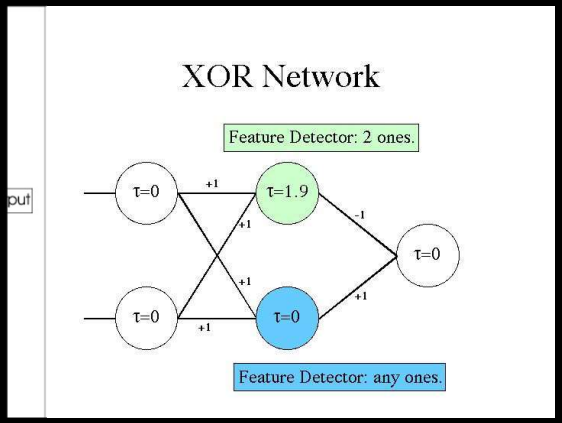


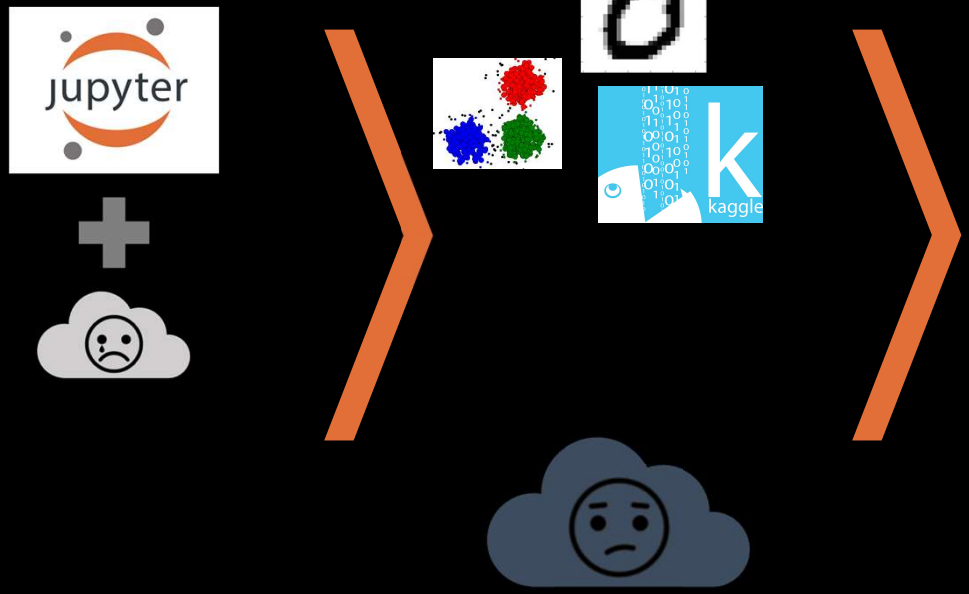
Figura 1
Modelo de um neurônio perceptron de Rosenblatt. Fonte: Adaptado de Medeiros (2006, p. 3).



#CODANDO

Usando a matemática para criar sua IA

Usando algoritmos e bases prontas para treinar



Nível de complexidade, ou ... quanto trabalho isso dá !!

Google Tensorflow e Mobilenet

IMAGENET

TensorFlow

https://github.com/tensorflow/tensorflow

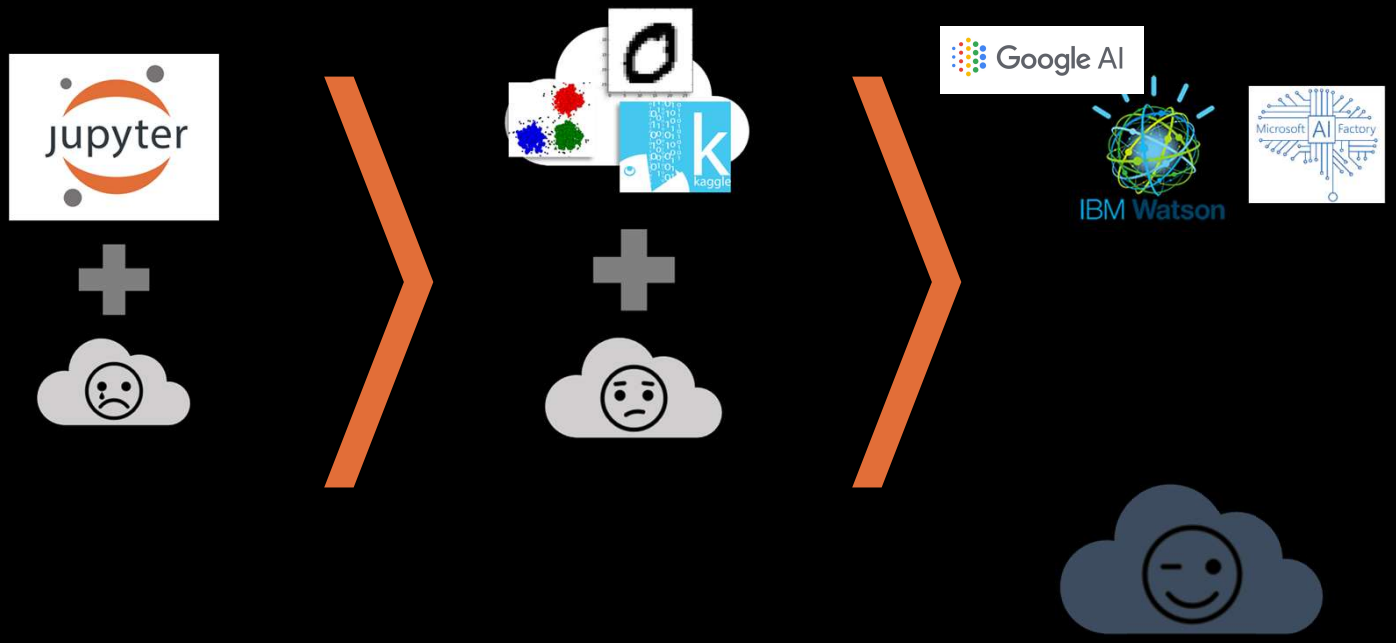
https://machinethink.net/blog/mobilenet-v2/

#CODANDO

Usando a matemática para criar sua IA

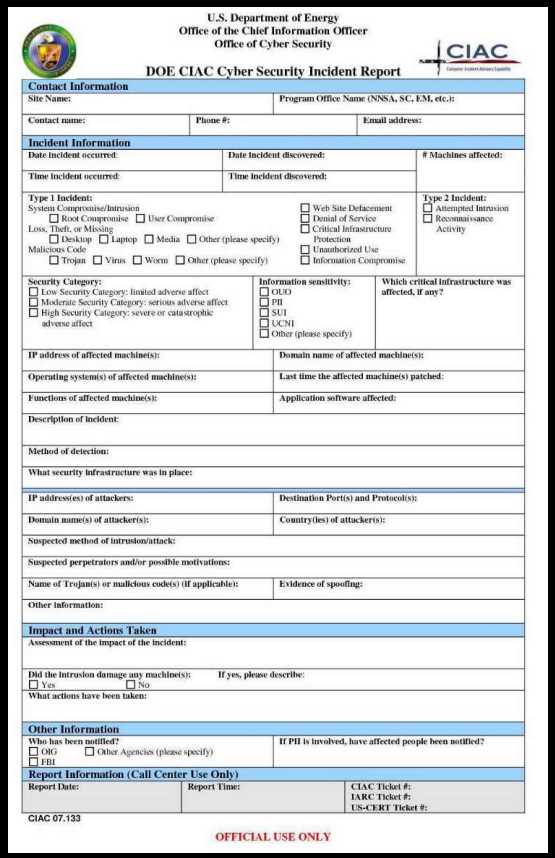
Usando algoritmos e bases prontas para treinar

Usando APIs e conhecimento do negócio



Nível de complexidade, ou ... quanto trabalho isso dá !!

Abrir incidente de segurança



U.S. Department of Energy
Office of the Chief Information Officer
Office of Cyber Security

DOE CIAC Cyber Security Incident Report

Contact Information

Site Name: | Program Office Name (NNSA, SC, EM, etc.):
Contact name: | Phone #: | Email address:

Incident Information

Date incident occurred: | Date incident discovered: | # Machines affected:
Time incident occurred: | Time incident discovered:

Type 1 Incident:
System Compromise/Intrusion
☐ Root Compromise ☐ User Compromise
Loss, Theft, or Missing
☐ Desktop ☐ Laptop ☐ Media ☐ Other (please specify)
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)
☐ Web Site Defacement
☐ Denial of Service
☐ Critical Infrastructure Protection
☐ Unauthorized Use
☐ Information Compromise

Type 2 Incident:
☐ Attempted Intrusion
☐ Reconnaissance Activity

Security Category:
☐ Low Security Category: limited adverse affect
☐ Moderate Security Category: serious adverse affect
☐ High Security Category: severe or catastrophic adverse affect

Information sensitivity:
☐ OUO
☐ PII
☐ SUI
☐ UCNI
☐ Other (please specify)

Which critical infrastructure was affected, if any?

IP address of affected machine(s): | Domain name of affected machine(s):
Operating system(s) of affected machine(s): | Last time the affected machine(s) patched:
Functions of affected machine(s): | Application software affected:
Description of incident:
Method of detection:
What security infrastructure was in place:

IP address(es) of attackers: | Destination Port(s) and Protocol(s):
Domain name(s) of attacker(s): | Country(ies) of attacker(s):
Suspected method of intrusion/attack:
Suspected perpetrators and/or possible motivations:
Name of Trojan(s) or malicious code(s) (if applicable): | Evidence of spoofing:
Other information:

Impact and Actions Taken

Assessment of the impact of the incident:
Did the intrusion damage any machine(s): ☐ Yes ☐ No | If yes, please describe:
What actions have been taken:

Other Information

Who has been notified?
☐ OIG ☐ Other Agencies (please specify)
☐ FBI
If PII is involved, have affected people been notified?

Report Information (Call Center Use Only)

Report Date: | Report Time: | CIAC Ticket #: IARC Ticket #: US-CERT Ticket #:

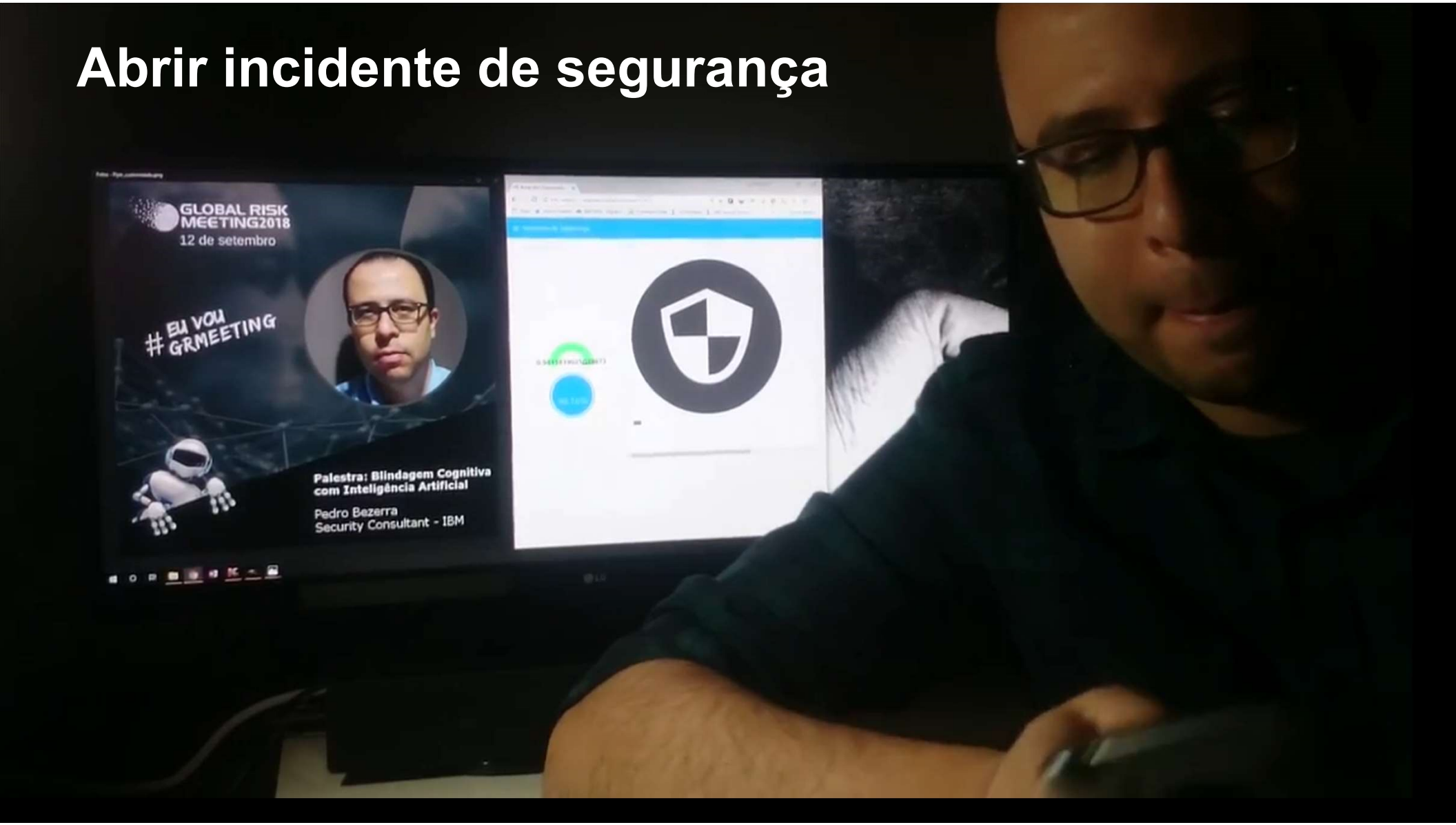
CIAC 07.133

OFFICIAL USE ONLY

Watson de Segurança

Fonte (Google): http://bardwellparkphysiotherapy.com

Abrir incidente de segurança



Fonte (Google): http://skillprogramming.com/recent/what-my-feeling-when-my-code-successful-work-3332


TELLO
Feel the Fun

Fontes:
www.youtube.com

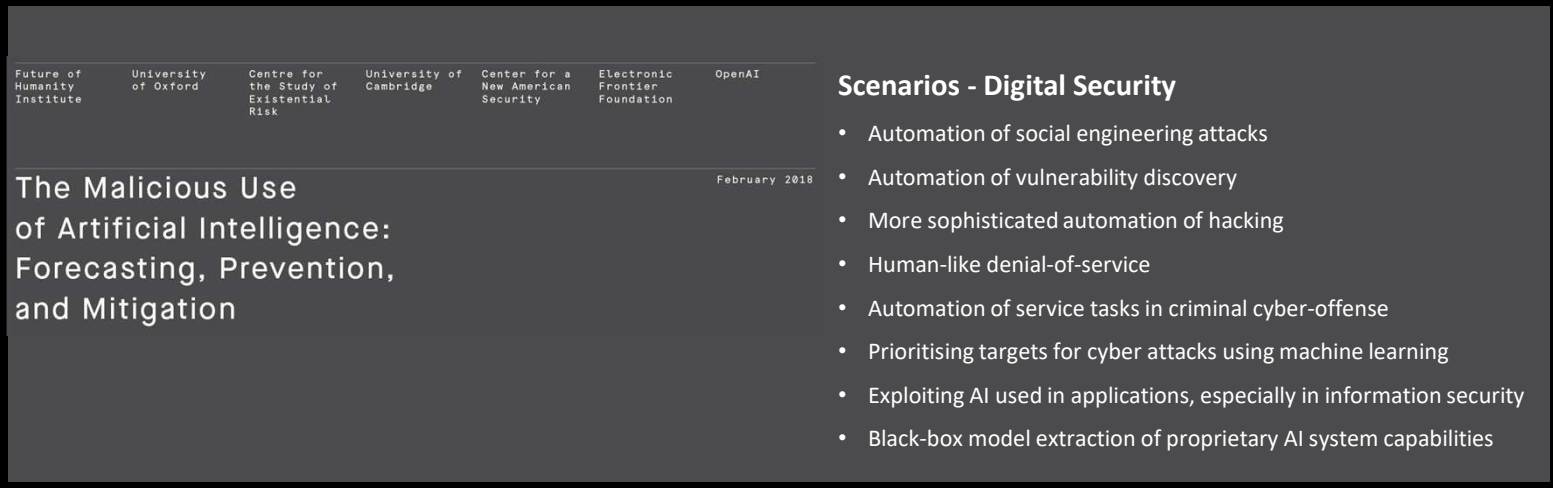
Fonte (Google): Stranger Things - NetFlix

Fonte (Google): Stranger Things - NetFlix

Fonte (Google): Stranger Things - NetFlix

Como podemos minimizar os impactos negativos:

1. Colaboração para investigar, prevenir e mitigar possíveis usos maliciosos da IA.
2. Pesquisadores e engenheiros em inteligência artificial devem levar a sério a natureza de dupla utilização de seu trabalho.
3. As melhores práticas devem ser identificadas.
4. Procurar ativamente expandir a discussão desses desafios.



Casos de Uso

1. Profissionais de SOC podem atender mais chamados, com qualidade.

2. Aprendem recorrentemente com as análises de profissionais e relatórios de riscos.

3. Documentos processuais de segurança podem ser interpretados pela Inteligência Artificial.

4. Atividades de programação segura com leitura do código fonte e sugestão de correção por uma AI treinada em desenvolvimento seguro.

5. Gestão de risco contínua e escalável, visto que existe um aprendizado, reaprendizado, acesso a todos os riscos de negócio e técnicas de mitigação.

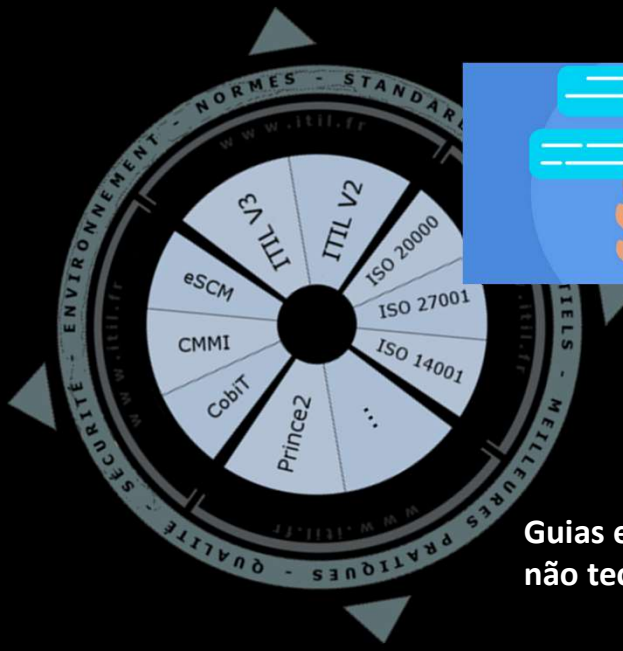
Protótipos

Abrir incidente de segurança por voz.

Node-Red

Watson Conversation

App Android



NLP tratando dados não estruturados

Guias e padrões não tecnológicos

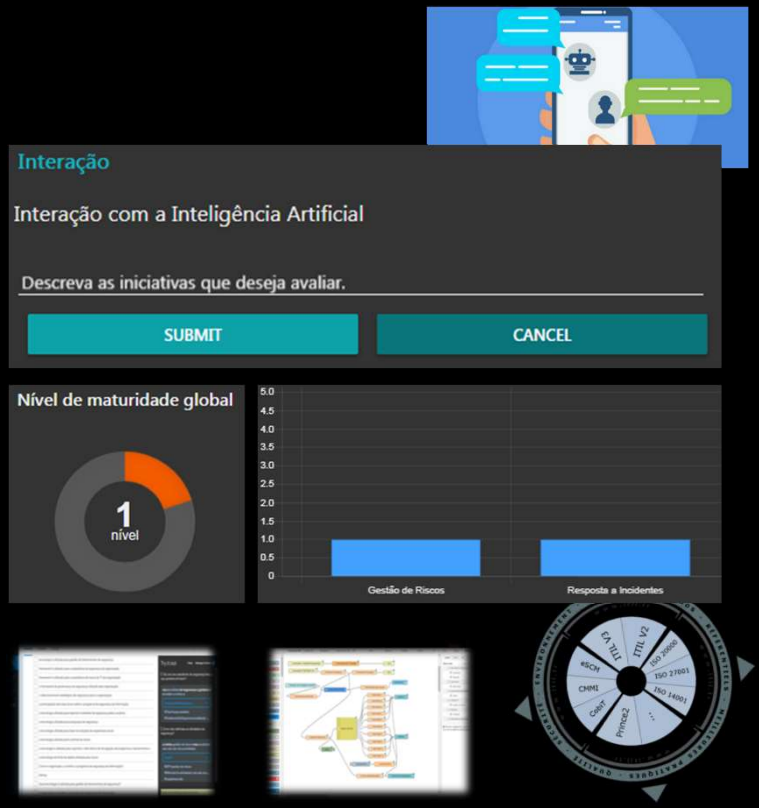
Protótipos

Inteligência Artificial que avaliação os processos de Segurança

Node-Red

Watson Conversation

App Android



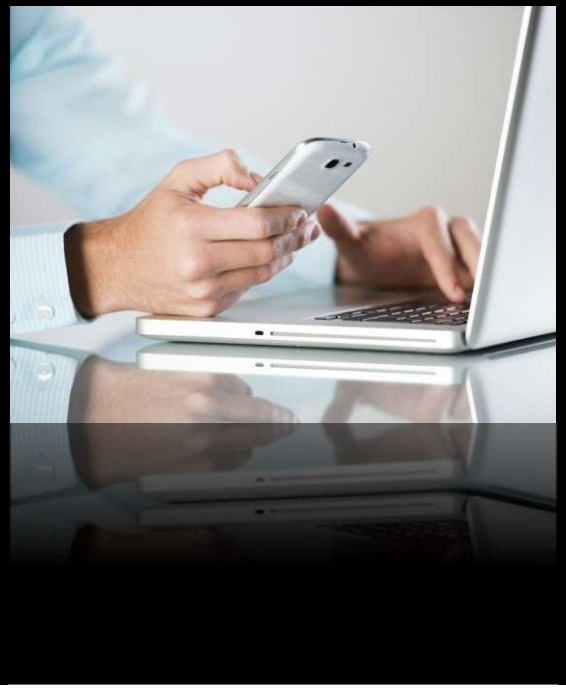
Protótipos

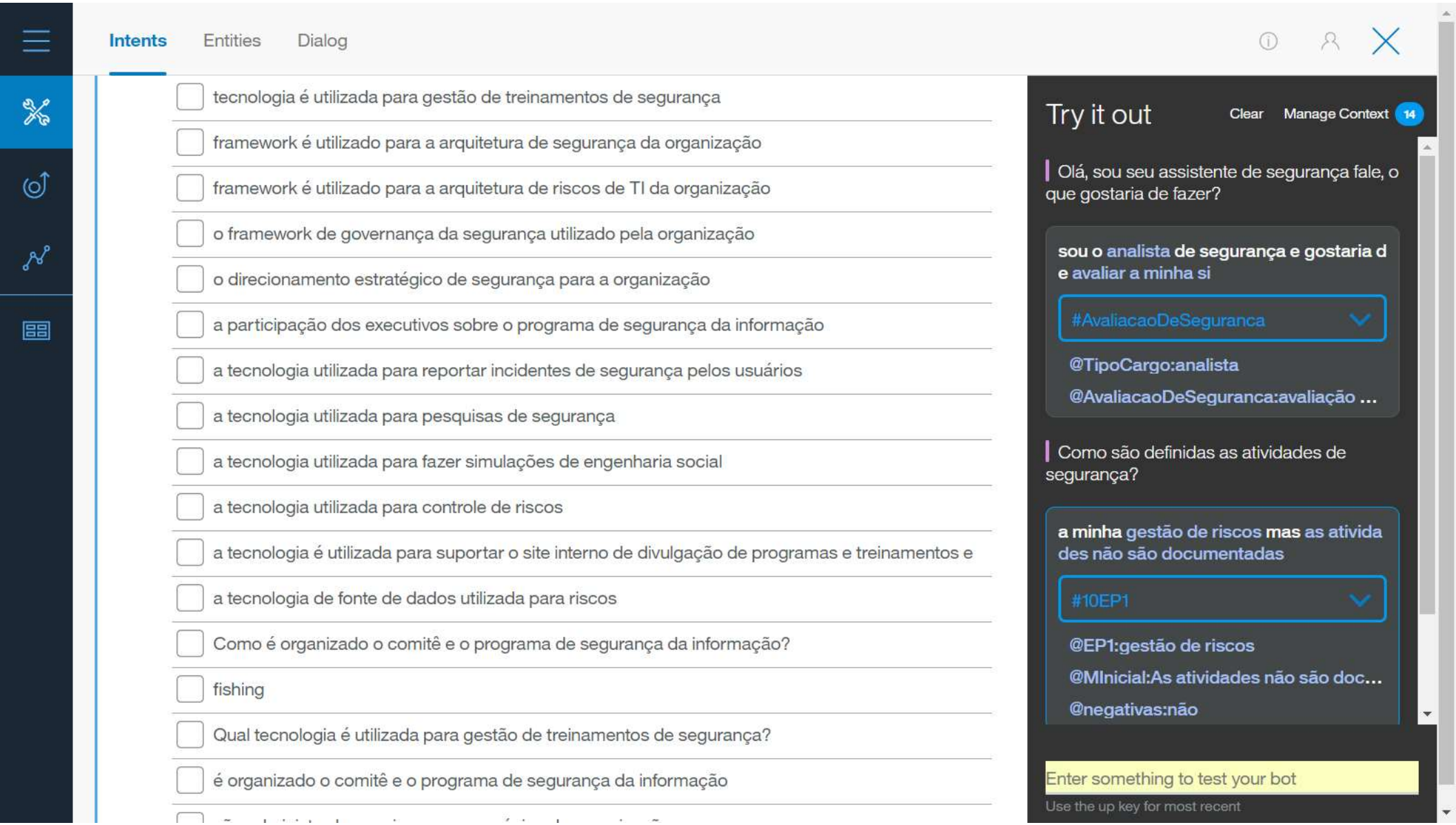
Inteligência Artificial
alertar
“vazamento de dados
por foto de celular”

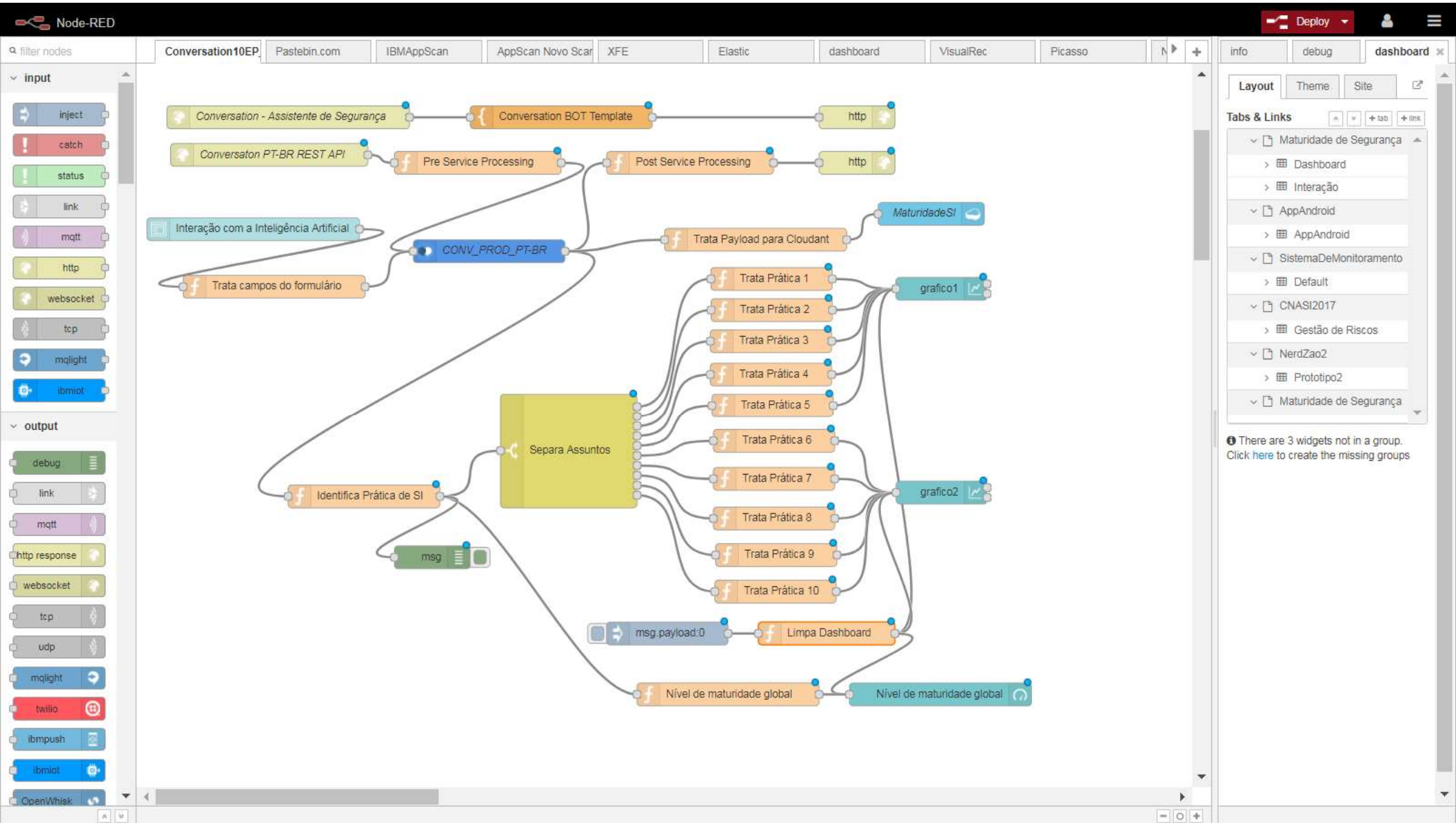
Watson Studio

Tensor Flow

Tensor Flow Mobile




Intents
Entities
Dialog
tecnologia é utilizada para gestão de treinamentos de segurança
framework é utilizado para a arquitetura de segurança da organização
framework é utilizado para a arquitetura de riscos de TI da organização
o framework de governança da segurança utilizado pela organização
o direcionamento estratégico de segurança para a organização
a participação dos executivos sobre o programa de segurança da informação
a tecnologia utilizada para reportar incidentes de segurança pelos usuários
a tecnologia utilizada para pesquisas de segurança
a tecnologia utilizada para fazer simulações de engenharia social
a tecnologia utilizada para controle de riscos
a tecnologia é utilizada para suportar o site interno de divulgação de programas e treinamentos e
a tecnologia de fonte de dados utilizada para riscos
Como é organizado o comitê e o programa de segurança da informação?
fishing
Qual tecnologia é utilizada para gestão de treinamentos de segurança?
é organizado o comitê e o programa de segurança da informação
Try it out
Clear
Manage Context
14
Olá, sou seu assistente de segurança fale, o que gostaria de fazer?
sou o analista de segurança e gostaria d e avaliar a minha si
#AvaliacaoDeSeguranca
@TipoCargo:analista
@AvaliacaoDeSeguranca:avaliação ...
Como são definidas as atividades de segurança?
a minha gestão de riscos mas as atividades não são documentadas
#10EP1
@EP1:gestão de riscos
@MInicial:As atividades não são doc...
@negativas:não
Enter something to test your bot
Use the up key for most recent


Node-RED
Deploy
Conversation10EP
Pastebin.com
IBMAppScan
AppScan Novo Scar
XFE
Elastic
dashboard
VisualRec
Picasso
info
debug
dashboard
Layout
Theme
Site
Tabs & Links
Maturidade de Segurança
Dashboard
Interação
AppAndroid
AppAndroid
SistemaDeMonitoramento
Default
CNASI2017
Gestão de Riscos
NerdZao2
Prototipo2
Maturidade de Segurança
There are 3 widgets not in a group.
Click here to create the missing groups
input
inject
catch
status
link
mqtt
http
websocket
tcp
mqlight
ibmiot
output
debug
link
mqtt
http response
websocket
tcp
udp
mqlight
twilio
ibmpush
ibmiot
OpenWhisk
Conversation - Assistente de Segurança
Conversation BOT Template
http
Conversaton PT-BR REST API
Pre Service Processing
Post Service Processing
http
Interação com a Inteligência Artificial
CONV_PROD_PT-BR
Trata Payload para Cloudant
MaturidadeSI
Trata campos do formulário
Trata Prática 1
Trata Prática 2
Trata Prática 3
Trata Prática 4
Trata Prática 5
Trata Prática 6
Trata Prática 7
Trata Prática 8
Trata Prática 9
Trata Prática 10
grafico1
grafico2
Separa Assuntos
Identifica Prática de SI
msg
msg.payload:0
Limpa Dashboard
Nível de maturidade global
Nível de maturidade global

security H1V3

AI Brasil
an artificial intelligence community

Perguntas ?

#FicaADica

Assine SLA de acurácia com o prestador de serviço de inteligência artificial, a tradicional CID não aborda nível de assertividade.

#Será?

Pequenos times de Segurança, utilizando ferramentas de IA, performam melhor que estruturas tradicionais ?

https://github.com/pedrohsbezerra
pedro.bezerra@outlook.com
Google: Pedro Bezerra GRC

Obrigado!