

DOGNÆDIS

TRUSTABLE SOLUTIONS

BE AT THE FOREFRONT
OF SECURITY TECHNOLOGIES

# HISTORY

CERT-IPN

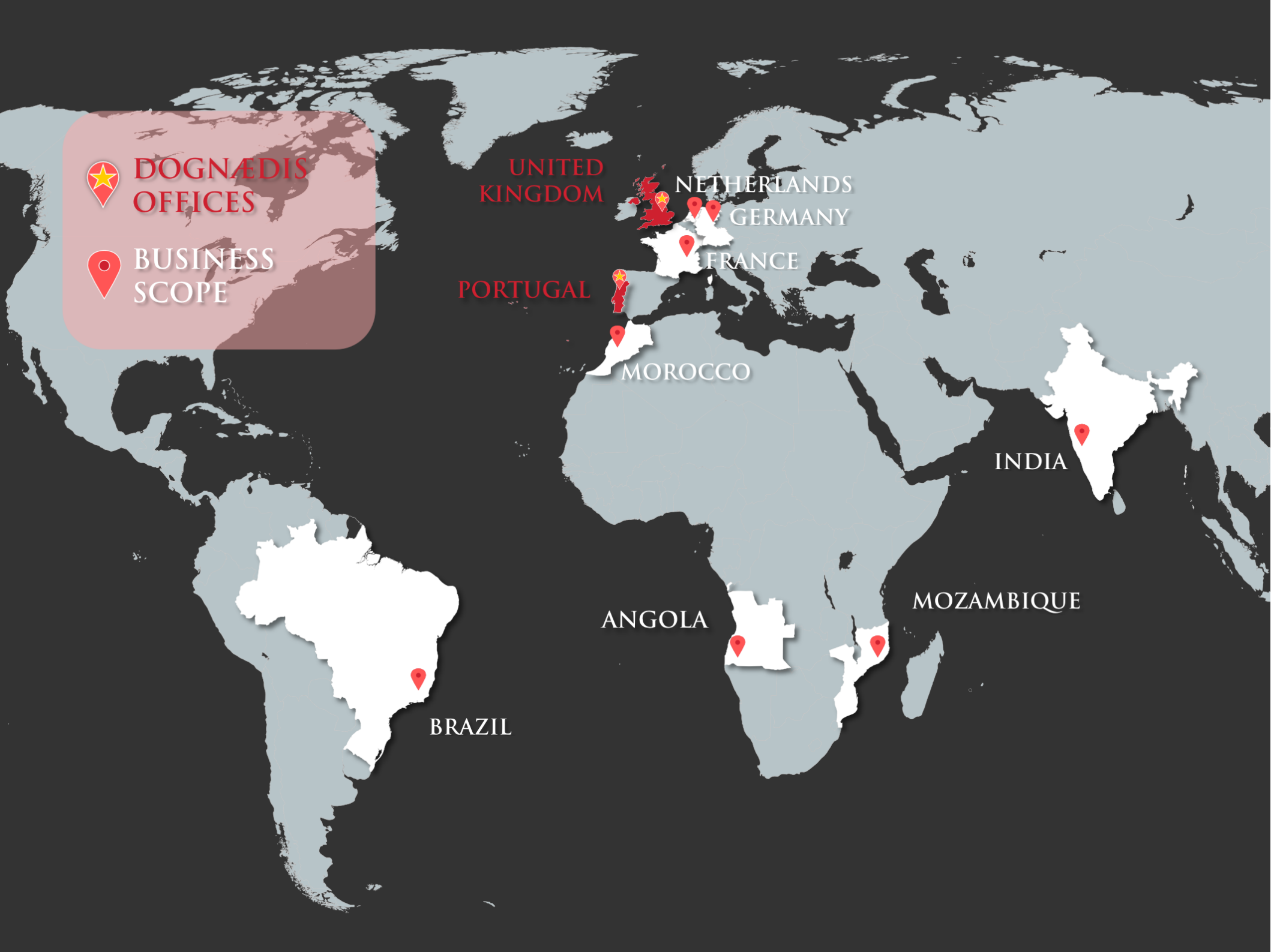
UNIVERSITY OF COIMBRA

DOGNÆDIS
TRUSTABLE SOLUTIONS

PROSEGUR

# AWARDS & CERTIFICATIONS

CERTIFIED BY
THE STANDARD
ISO/IEC 27001
ISO/IEC 9001


DOGNÆDIS OFFICES
BUSINESS SCOPE
UNITED KINGDOM
NETHERLANDS
GERMANY
FRANCE
PORTUGAL
MOROCCO
INDIA
ANGOLA
MOZAMBIQUE
BRAZIL


TELCO & IT
40%


FINANCIAL
30%


DEFENSE
10%


GOVERNMENT
20%

# Estado de Alerta

Indicadores para a Segurança do dia a dia

ampp@dognaedis.com

André Pinheiro

Abril 2016

# Dognædis

Dedicada à Segurança de Informação

Inicia atividade a partir de um CERT

# Resposta a Incidentes

Acção ou acções que ajudem a mitigar ou diminuir os impactos para a organização de um determinado acontecimento.

# Situational Awareness

Perceção dos elementos que nos rodeiam para um determinado espaço e tempo. A capacidade de compreender a informação disponível  projetando cenários futuros com a informação disponível.

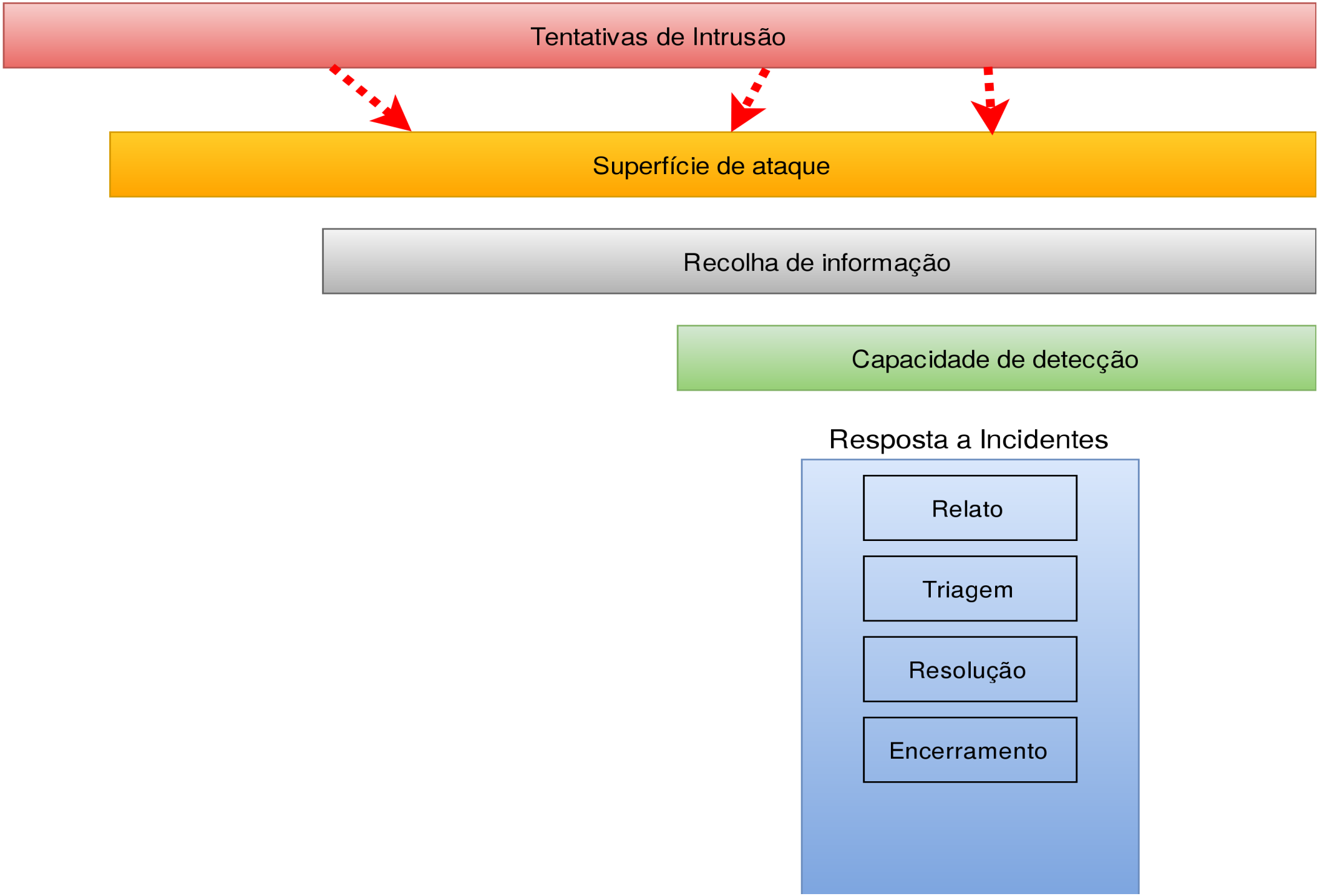
# *SA* no ciclo de *IH*

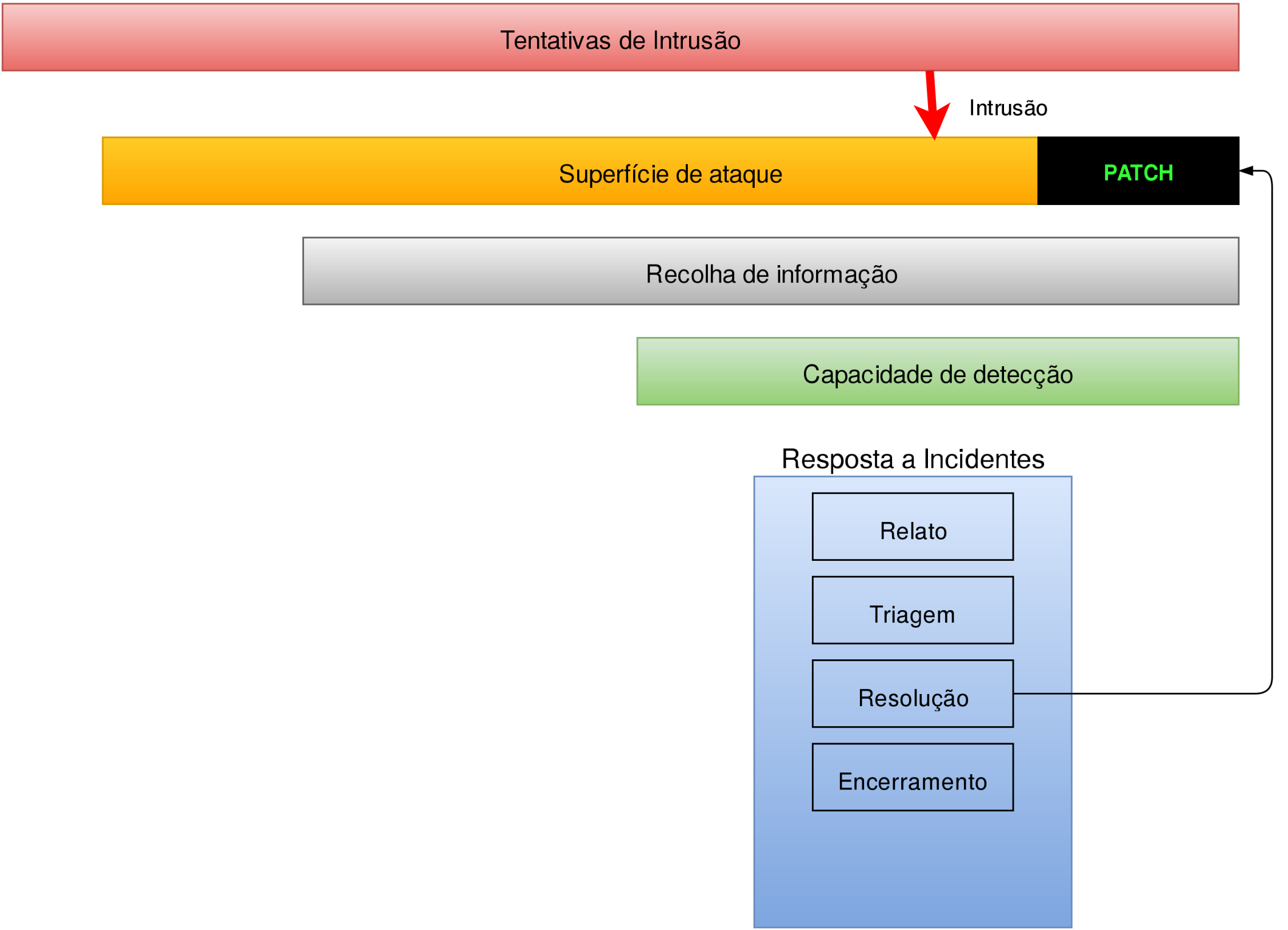
Torna a resposta pro-ativa

Interage com *VA*

Requer informação interna e externa

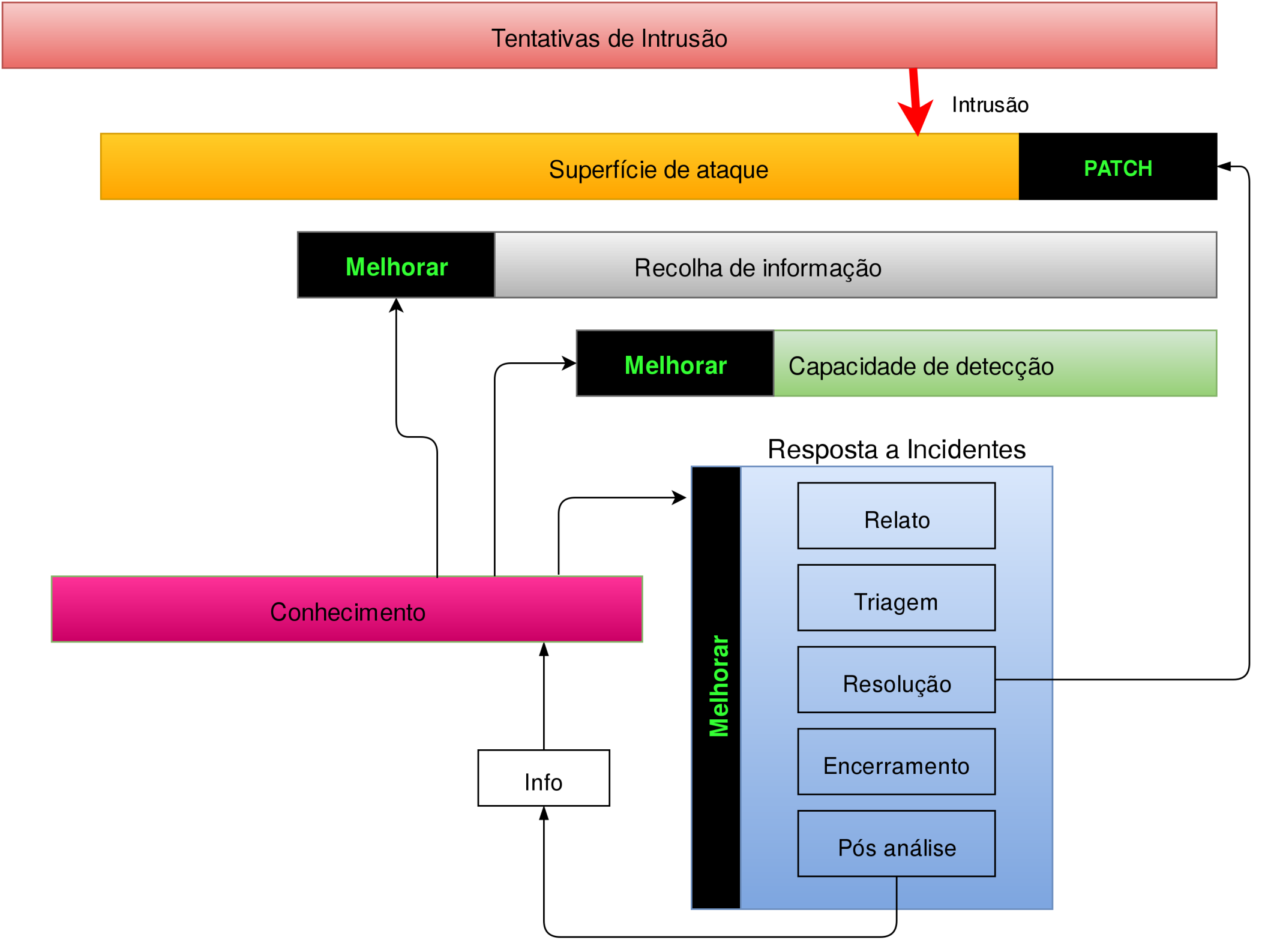
Dependente da missão


Tentativas de Intrusão
Superfície de ataque
Recolha de informação
Capacidade de detecção
Resposta a Incidentes
Relato
Triagem
Resolução
Encerramento


Tentativas de Intrusão
Intrusão
Superfície de ataque
PATCH
Recolha de informação
Capacidade de detecção
Resposta a Incidentes
Relato
Triagem
Resolução
Encerramento

# Como melhorar?

Estamos a aprender com a situação?

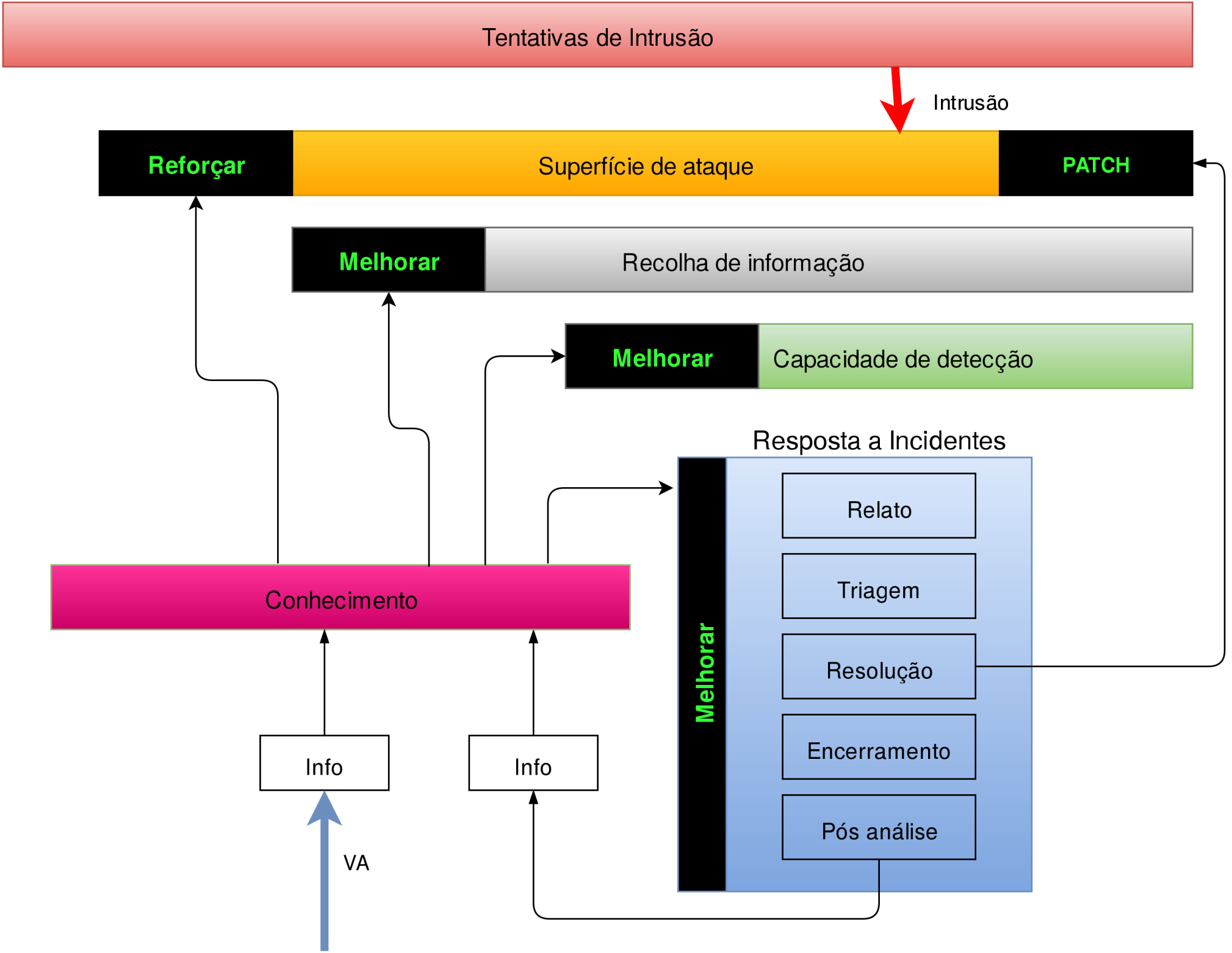

Tentativas de Intrusão
Intrusão
Superfície de ataque
PATCH
Melhorar
Recolha de informação
Melhorar
Capacidade de detecção
Resposta a Incidentes
Melhorar
Relato
Triagem
Resolução
Encerramento
Pós análise
Conhecimento
Info

# VA?

Como se encaixa no ciclo?

Apenas atuamos sobre ativos atacados

Classificação de ativos


Tentativas de Intrusão
Intrusão
Reforçar
Superfície de ataque
PATCH
Melhorar
Recolha de informação
Melhorar
Capacidade de detecção
Resposta a Incidentes
Melhorar
Relato
Triagem
Resolução
Encerramento
Pós análise
Conhecimento
Info
Info
VA

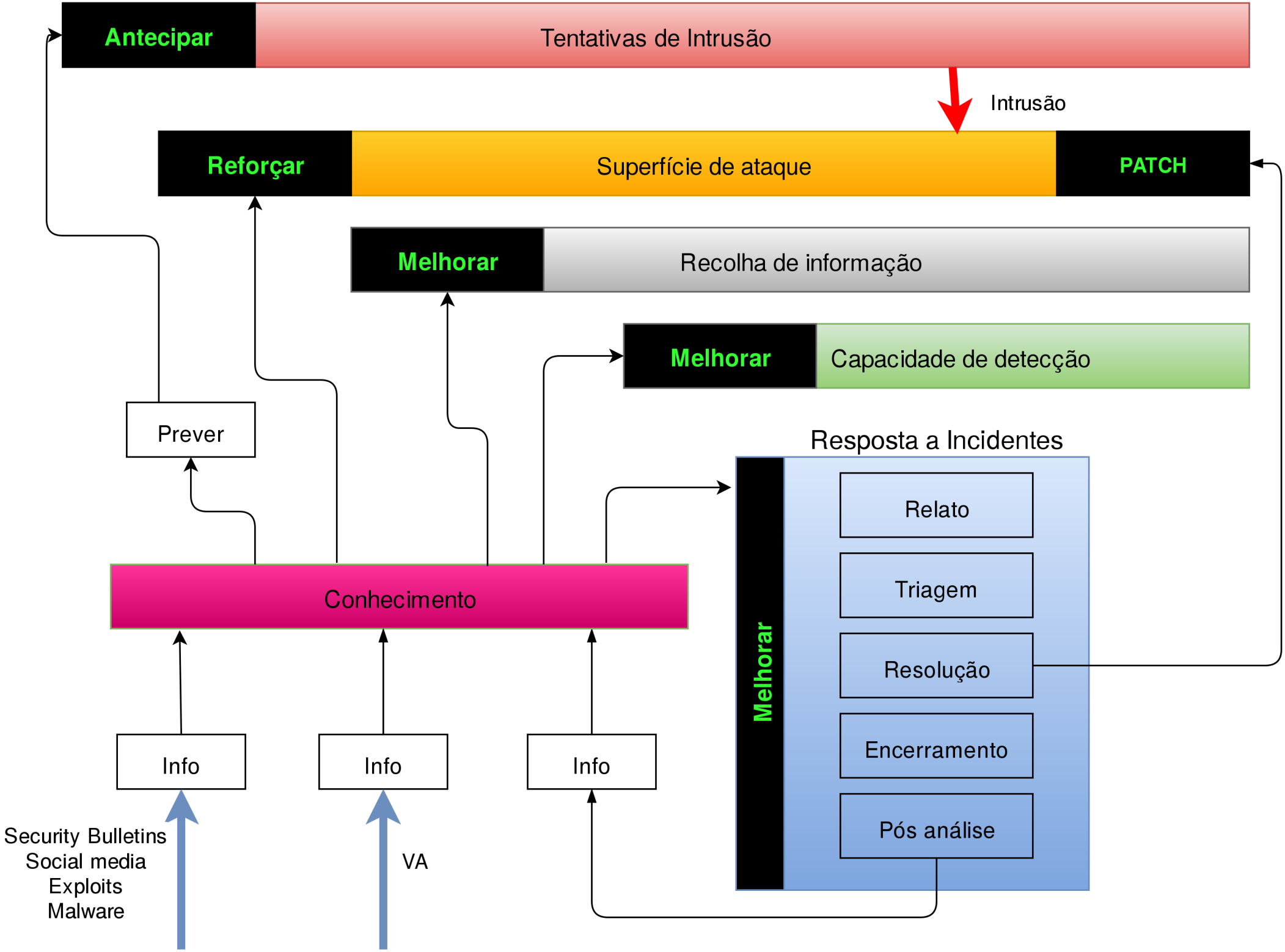
# Estamos alerta?

Temos conhecimento interno

Conhecemos as nossas vulnerabilidades

Continuamos a reagir aos ataques

Não estamos conscientes do que está “lá fora”


Antecipar
Tentativas de Intrusão
Intrusão
Reforçar
Superfície de ataque
PATCH
Melhorar
Recolha de informação
Melhorar
Capacidade de detecção
Prever
Resposta a Incidentes
Relato
Triagem
Resolução
Encerramento
Pós análise
Melhorar
Conhecimento
Info
Info
Info
Security Bulletins
Social media
Exploits
Malware
VA

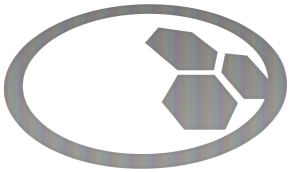
# Cyber Intelligence

Fulcral para atingir o *SA*

Informação a recolher consistente com a missão

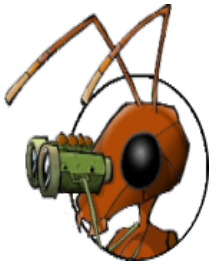
Fontes diversas

Grande quantidade de informação



astaro
Sophos Network






























# Como tratar?

Uniformizar

Centralizar

Indexar

Interface de pesquisa



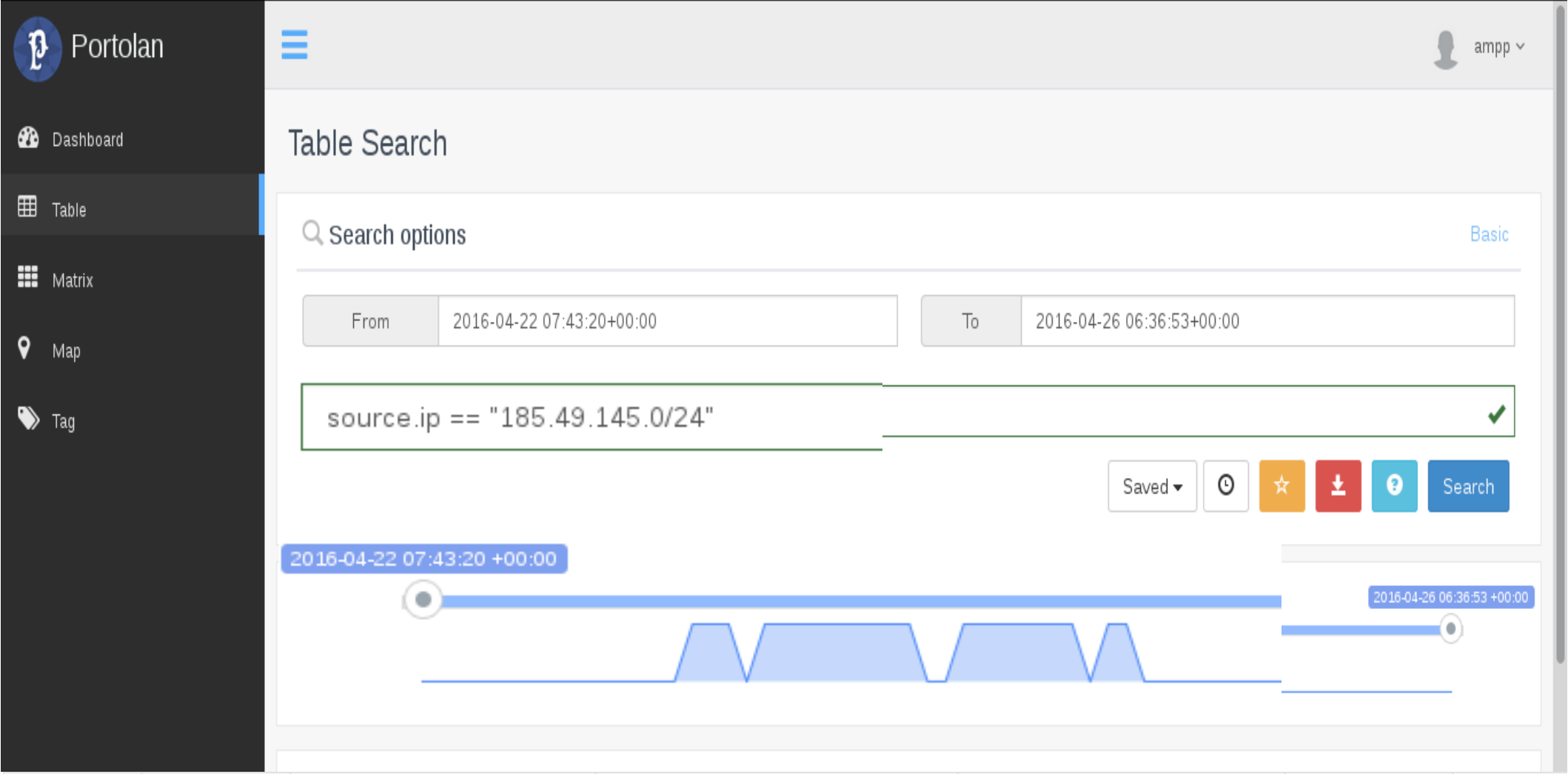
PORTOLAN

Making decision an instinct

# Exemplo 1

Alerta “Scan + Brute force”

IP: 185.49.145.70




| Type | Feed ID | IP Address (Source) | IP Address (Destination) | Observation Time | TAGS | Action |
|---|---|---|---|---|---|---|
| malware | autoshun | 185.49.145.71 | *Unknown* | April 23, 2016 10:46:31 | IPAddress | |
| malware | autoshun | 185.49.145.73 | *Unknown* | April 23, 2016 10:46:31 | IPAddress | |
| malware | autoshun | 185.49.145.70 | *Unknown* | April 23, 2016 10:46:31 | IPAddress | |
| malware | autoshun | 185.49.145.72 | *Unknown* | April 23, 2016 10:46:31 | IPAddress | |
| malware | autoshun | 185.49.145.74 | *Unknown* | April 23, 2016 10:46:31 | IPAddress | |
| malware | autoshun | 185.49.145.70 | *Unknown* | April 23, 2016 11:46:33 | IPAddress | |
| malware | autoshun | 185.49.145.71 | *Unknown* | April 23, 2016 11:46:33 | IPAddress | |
| malware | autoshun | 185.49.145.72 | *Unknown* | April 23, 2016 11:46:33 | IPAddress | |

# Abordagem

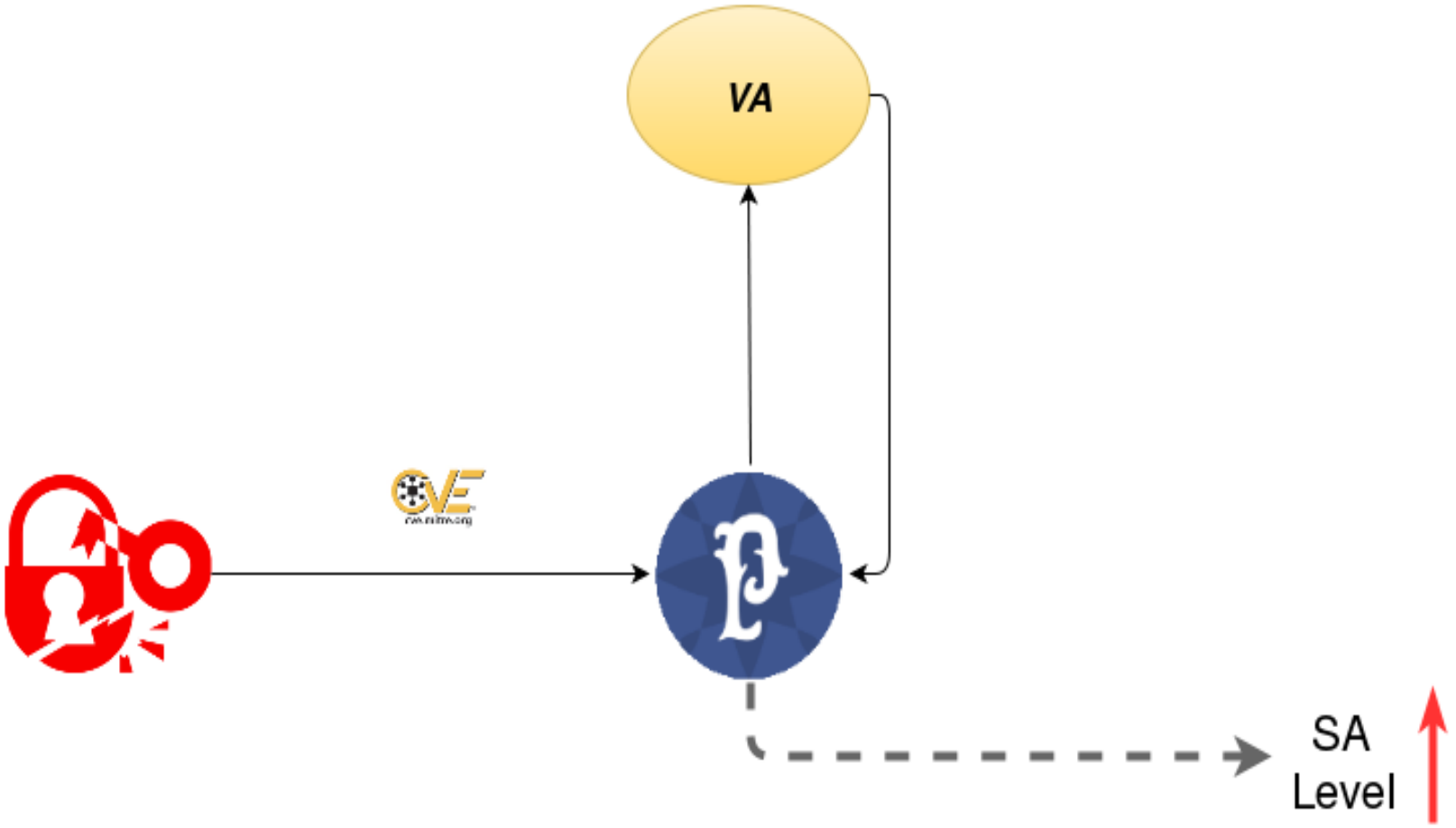
Identificação do atacante

Identificação de outros endereços

Bloqueio do IP atacante e outros identificados

# Exemplo 2




VA
SA
Level

# Abordagem

Verificar razão do aumento do *SA*

Auditar todas as contas de domínio

Mapear todos os administradores

Impedir escalada de privilegio

Mais monitorização nas operações ao *AD*

Aumentar os recursos da equipa

# *SA* como indicador

Capacidade de filtragem da informação

Visão interna e externa

Alinhar com a missão da organização

Criar uma escala

Mudança de nível despoleta ações

# Resumo

Visão Interna

Visão Externa (*Cyber Intelligence*)

Novo ciclo de *IH*

Indicador de *Situation Awareness*

# DOGNÆDIS

## TRUSTABLE SOLUTIONS




+351 239 047 756



info@dognaedis.com



www.dognaedis.com

PT



Rua do Brasil
Edifício n.º 2
n.º 239 - 3º Esq.
3030-175 Coimbra

UK



Innovation Centre
Gallows Hill
Warwick
CV34 6UW

US



West Pickle
Research
Building, 3925
West Braker
Lane, Austin,
Texas 78759