MICROSEGUR
Soluções integradas de tecnologia e segurança

DESAFIOS E INSTRUMENTOS DE PROTEÇÃO DE INFRAESTRUTURAS CRÍTICAS

MICROSEGUR

INSPEÇÃO - HS

- ✓ Pessoas
- ✓ Correio
- ✓ Bagagem
- ✓ Carga
- ✓ Explosivos e Narcóticos

SIA

- ✓ SADI
- ✓ CCTV
- ✓ SACA
- ✓ PSIM
- ✓ SADIR

IOT & IIOT

- ✓ Smart Office
- ✓ Smart Building
- ✓ RTLS
- ✓ Indústria 4.0

DRONES

- ✓ Sistemas Antidrones
- ✓ Vigilância Autónoma
- ✓ Inspeção de Infraestruturas
- ✓ Mapeamento 3D

REDES

- ✓ Infraestruturas (Shelters, FO, Datacenters, etc.)
- ✓ Equipamentos passivos
- ✓ Equipamentos activos

SOLUÇÕES ESPECIAIS

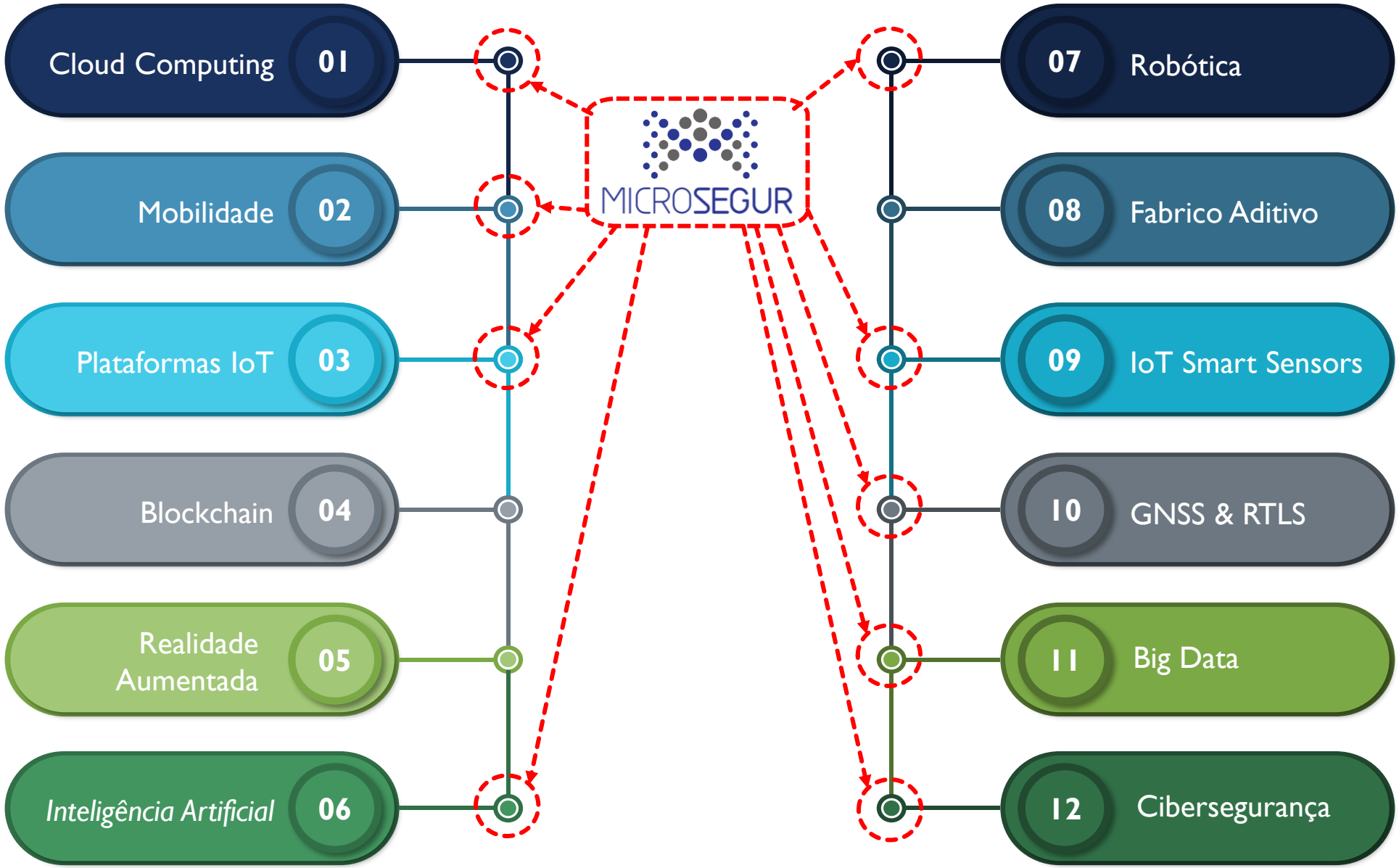
- ✓ Monitorização pipelines com FO.
- ✓ Deteção de Fraude
- ✓ Sistema de Proteção à Vitima

ISO 9001
Desde 2008

NATO/OTAN Secret
Desde 2010

Secreto
Desde 2009

A Microsegur e as tecnologias que impulsionam a Transformação Digital



RISCOS / AMEAÇAS

COMO DIMINUIR O RISCO NAS INFRAESTRUTURAS CRITICAS?

How a 5G coronavirus conspiracy spread across Europe | Free to read

Nic Fildes and Mark Di Stefano in London and Hannah Murphy in San Francisco - APRIL 16 2020

At about 9.30pm on Easter Monday, in the small Dutch town of Almere near Amsterdam, the fire brigade was called to put out a blaze at a large telecoms mast — the second fire of its kind that night in the area.

Though neither of the Almere towers were equipped with any of the latest 5G telecoms equipment — in fact one was designed only for use by the emergency services — authorities soon concluded that the fires were perpetrated by vandals acting in the name of an **unusual theory: that 5G networks have contributed to the coronavirus pandemic**…

Spate of arson attacks on telecoms masts fuelled by disinformation over pandemic's origins

In the UK, conspiracy theories have even seeped on to mainstream TV, alarming broadcasters and Ofcom © Neil Hall/EPA/Shutterstock

https://www.ft.com/content/1eeedb71-d9dc-4b13-9b45-fcb7898ae9e1

Multiple fibers cut across France, impacting several cities

Cables connecting Paris to the cities of Lyon, Strasbourg, and Lille cut in several places

April 27, 2022 By: Dan Swinhoe Comment

A number of fiber optic cables across France have seemingly been intentionally cut, causing Internet outages and slowdowns in cities across the country.

Cables connecting Paris to the cities of Lyon, Strasbourg, and Lille were physically cut in several places.

"Internet cables have been cut in the Ile-de-France region, which is affecting the landline and mobile network. We are in touch with operators who are working to restore service," Minister for digital affairs Cedric O said in a tweet.

French media reported major internet outages in cities including Paris, Lyon, Bordeaux, Reims and Grenoble…

https://www.datacenterdynamics.com/en/news/multiple-fibers-cut-across-france-impacting-several-cities/

enisa

EUROPEAN UNION AGENCY FOR CYBERSECURITY

Guideline on Threats and Assets

Technical guidance on threats and assets in Article 13a

V1.0, January 2015

"…In this document, we provide guidance to National Regulatory Authorities (NRAs) about the risk assessment mentioned in paragraphs 1 and 2 of Article 13a of the Framework directive (Directive 2002/21/EC as amended by Directive 2009/140/EC)..."

Domínio Cibernético

Domínio Fisico

- Heavy snow and ice
- Heavy wind
- Flood
- Earthquake
- Wildfire
- Fire
- Explosion
- Arson
- Electromagnetic interference
- Denial of service attack
- Network traffic hijack
- Malware attack
- Hardware theft
- Cable theft
- Cable cut
- Power cut
- Power surge
- Cooling outage
- Hardware failure
- Sofware bug
- Faulty hardware change/update
- Faulty software change/update
- Overload
- Fuel exhaustion
- Policy or procedure flaw

https://resilience.enisa.europa.eu/article-13/guideline_on_threats_and_assets/Article_13a_Guideline_on_Threats_and_Assets_V_1_0.pdf

DOMINIO CIBERNÉTICO

RELATÓRIO ENISA SOBRE O

CENÁRIO DAS AMEAÇAS DE 2021

Abril de 2020 a meados de julho de 2021

enisa

EUROPEAN UNION AGENCY FOR CYBERSECURITY

DOMINIO CIBERNÉTICO

- O software de sequestro foi avaliado como sendo a principal ameaça de 2020-2021.
- As organizações governamentais intensificaram os seus esforços ao nível nacional e internacional.
- Os cibercriminosos estão cada vez mais motivados pela monetização das suas atividades, por exemplo, o software de sequestro. A criptomoeda continua a ser o método de pagamento mais comum entre os perpetradores.
- O declínio do software malicioso observado em 2020 mantém-se em 2021. Em 2021, observou-se um aumento do número de perpetradores que recorreram a linguagem de programação relativamente nova ou invulgar para veicular o seu código.
- O volume de infeções por criptossequestro atingiu um nível recorde no primeiro trimestre de 2021, comparativamente aos últimos anos. Os ganhos financeiros associados ao criptossequestro incentivaram os perpetradores a levarem a cabo estes ataques.
- A COVID-19 é o engodo dominante nas campanhas para ataques de correio eletrónico.
- Registou-se um aumento substancial das violações de dados no setor da saúde.
- As tradicionais campanhas de DDoS (ataques distribuídos de negação de serviço) em 2021 foram mais direcionadas, mais persistentes e cada vez mais multivetoriais. A IoT (Internet das coisas), em conjunto com as redes móveis, está a causar uma nova onda de ataques de DDoS.
- Em 2020 e 2021, observou-se um aumento significativo dos incidentes não maliciosos, já que a pandemia de COVID-19 se tornou num multiplicador de erros humanos e falhas de configuração dos sistemas, ao ponto de a maioria das violações em 2020 terem sido causadas por erros.

RELATÓRIO ENISA SOBRE O CENÁRIO DAS AMEAÇAS DE 2021 Abril de 2020 a meados de julho de 2021

	4/20	5/20	6/20	7/20	8/20	9/20	10/20	11/20	12/20	1/21	2/21	3/21	4/21	5/21	6/21	7/21	Total
Water utilities	1	1	1	1													**4**
Transport	3	2	2	1	2	2	7	2	3	4	1	7	4	5	4	5	**54**
Targeted individuals			1	1	1	3	2	1	1	1	6	3	4	2	5	2	**33**
Space	1		2	1							1						**5**
Software supply chain			4			1	1		4	5	3	2	5	5	1	4	**35**
Semiconductor						1											**1**
Public administration/ Government	2	7	20	5	13	14	14	8	10	4	10	12	18	19	21	21	**198**
Postal & Courier Services											1	2		3			**6**
Military		2	8	1	6	1	1	1			3	4	1	3	3	1	**35**
Media/Entertainment		1	1	2	1	3	2	2	3	2	3	1	2	3	5	2	**33**
Legal		2					1	1				1	3		1		**9**
Healthcare/Medical	1	5	7	5	3	5	7	8	10	5	11	7	5	29	19	16	**143**
General public	13	21	15	16	8	12	7	6	3	5	7	9	8	13	7	1	**151**
Food												1	3	7	5		**16**
Finance/Banking	2	6	4	10	2	12	1	2	6	7	6	8	7	6	9	9	**97**
Energy	4	4	4	1		1	1	3	1	2	1	3	1	2	3	2	**33**
Education/Academic	2	2	5	2	4	6	2	1	1	2	3	6	8	5	3		**52**
Digital Service Providers	1		7	8	8	9	6	9	6	14	22	11	13	10	18	10	**152**
Construction		6	5	1	1	1		2	1	1	1	2	2	2	1	4	**30**
All Sectors			3		3		1		1	2	11	10	4	6	5	1	**47**

DOMINIO FISICO

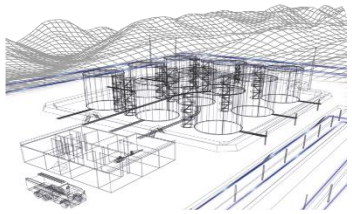
SOLUÇÕES SEGREGADAS

- Deteção de intrusão
- Controlo e gestão de acessos
- Videovigilância
- Inspeção Pessoas e Bagagens
- Deteção de Incêndio
- Monitorização Consumo e Disponibilidade de Energia

DOMINIO FISICO
INTRUSÃO

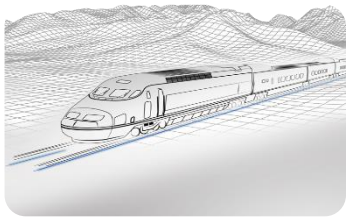
- Monitorização de Infraestruturas lineares através de interrogarores sobre fibra negra
  - Monitorização de intrusão com classificação do tipo de ameaça (Pessoas, Viaturas, Escavação, etc)
  - Deteção de Fugas (através de 4 indicadores: ruído do orifício, pulso de pressão negativa, tensão ambiental (elevação do solo) e deteção de gradiente de temperatura distribuída.
  - Deteção de movimentos do solo (sismos, deslizes, abatimentos, etc.)
  - Tracking de equipamentos de inspeção.

OUTRAS APLICAÇÕES



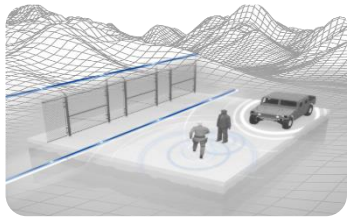
Perímetros

- Deteta, localiza e classifica várias ameaças
- Classifica veículos, pessoas;
- Classifica atividades de escavação e violação de cercas;
- Integra com sistemas de videovigilância para controlo automático das camaras



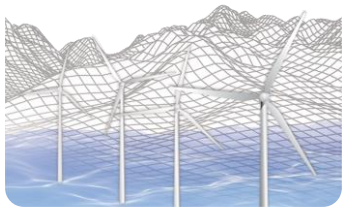
Caminhos de Ferro

- Detecção de intrusão e das atividades associadas ao roubo de cabo;
- Deteção de queda de rochas e deslize de terras;
- Tracking da posição das composições;
- Detecção de anomalias comuns de das linhas e material circulante, como defeitos nas rodas e nos carris.



Fronteiras

- Deteta, localiza e classifica várias ameaças
- Classifica veículos, pessoas;
- Classifica atividades de escavação e violação de cercas
- Integra com sistemas CCTV para control automático das camaras



Energia

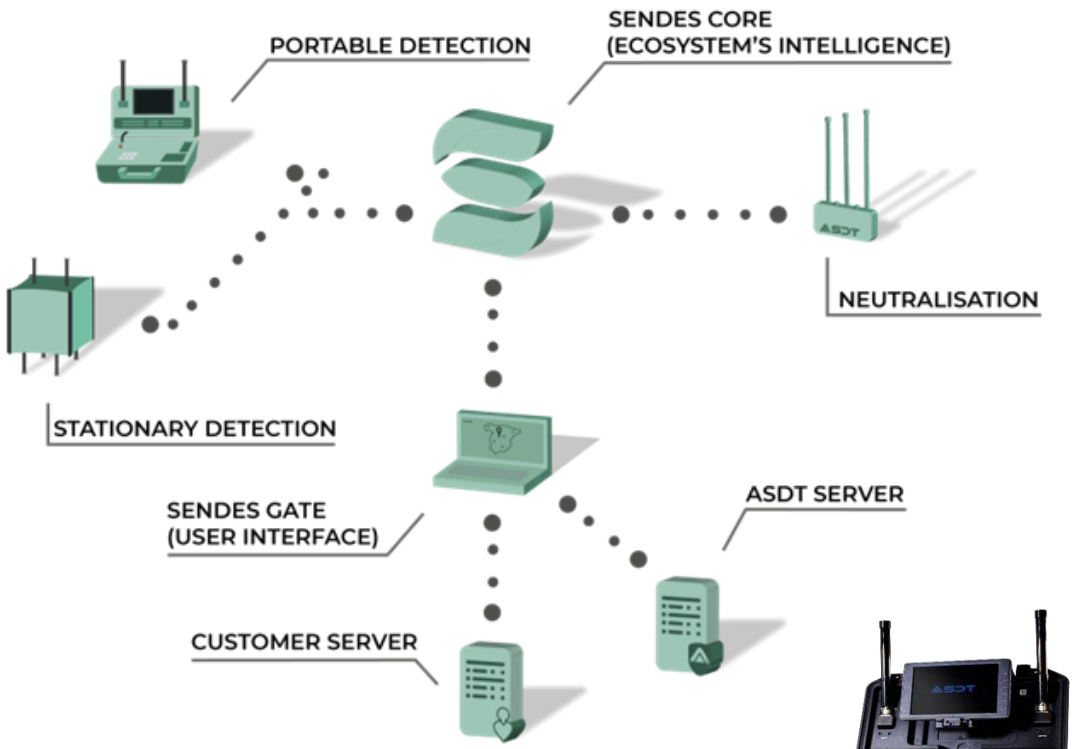
- Deteta e localiza falhas nos cabos, as mudanças de temperatura;
- Deteta ondas de choque para localizar curtos-circuitos em tempo real;
- Deteta e classifique intrusão e classifica atividades, como escavação manual ou mecânica e roubo;
- Antecipa falhas de cabo caras através da escuta dos indicadores acústicos de desempenho funcional.

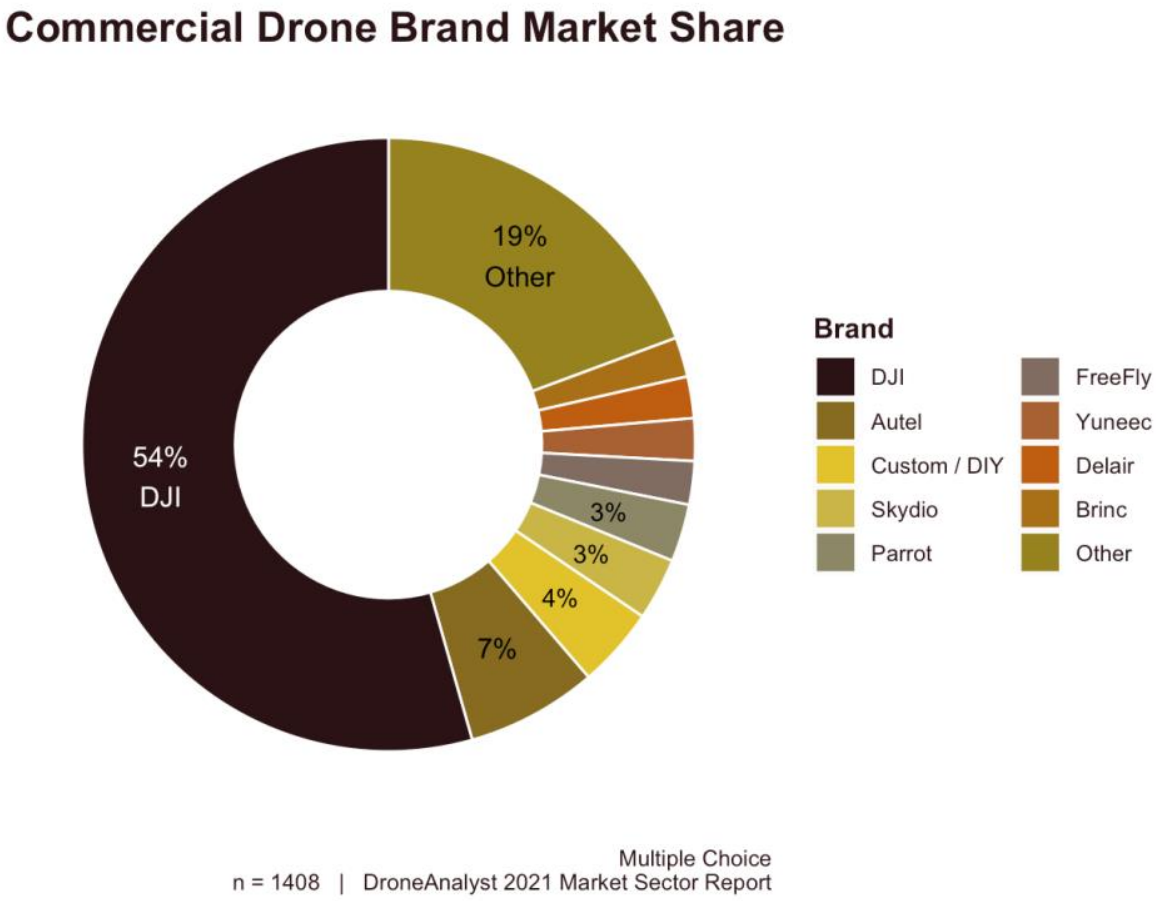
Vigilância

Câmaras com Video Analítico

Radares

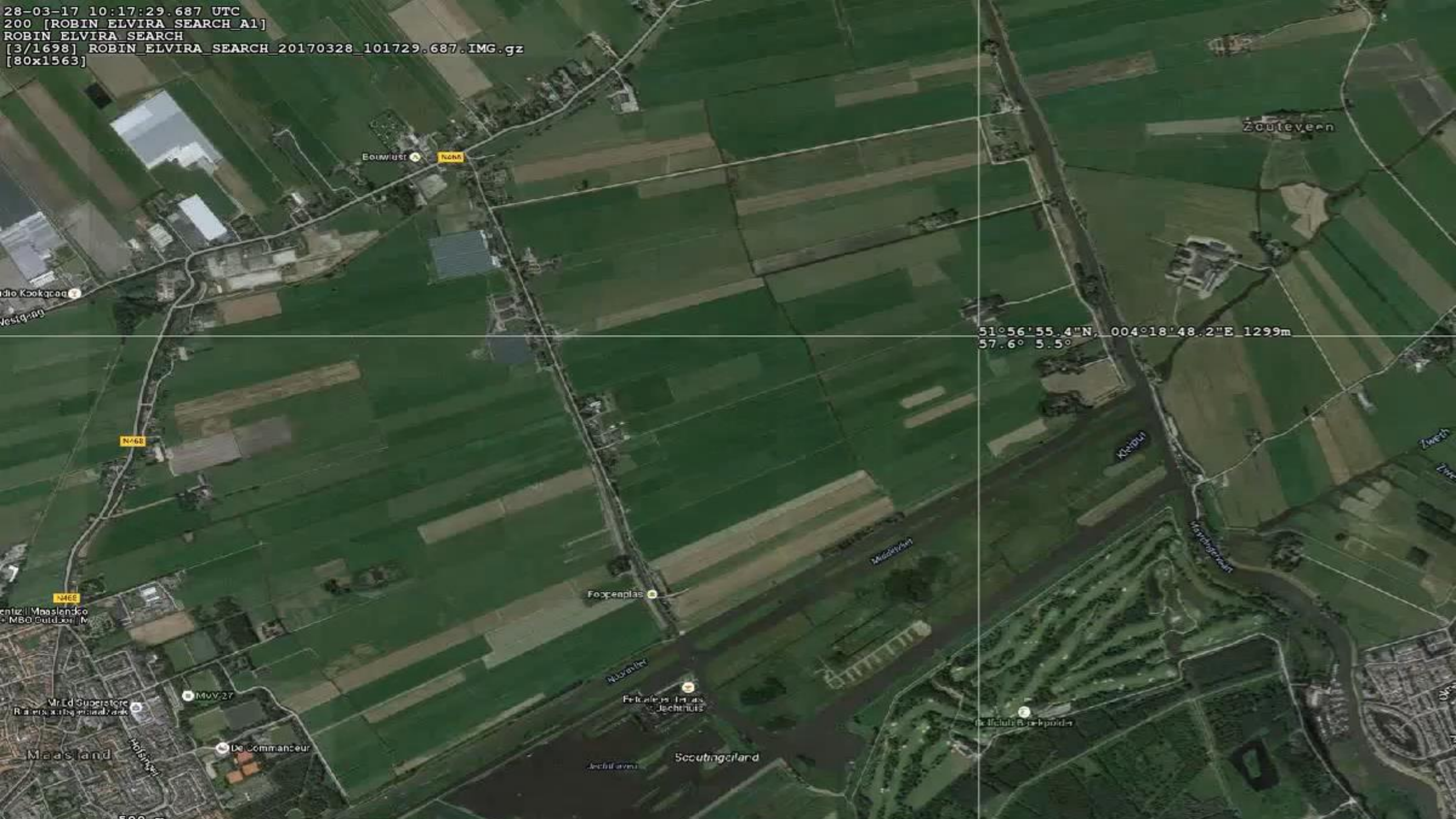
Sistemas de deteção de Drones:



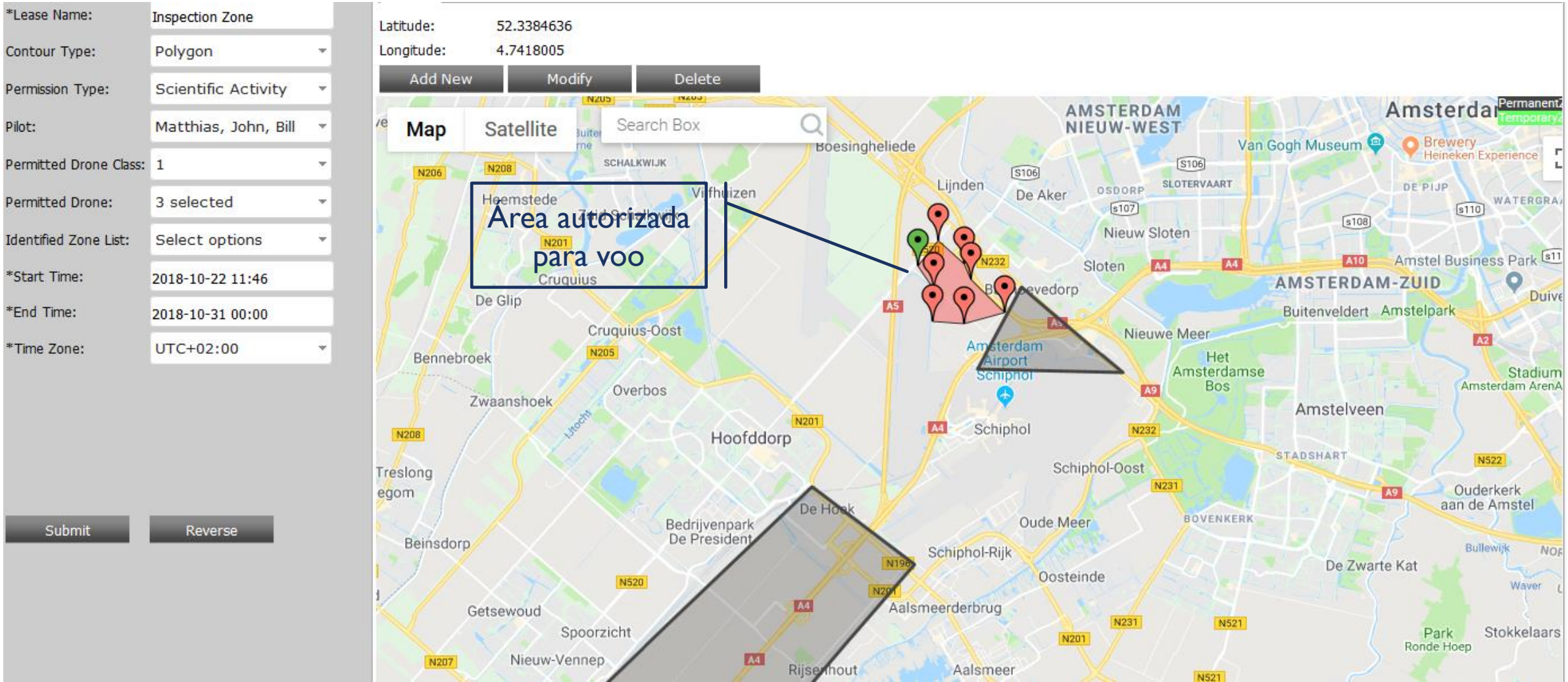


U.S. Department of Homeland Security
25.5K subscribers

https://www.youtube.com/watch?v=o6x-cj1wXZk


28-03-17 10:17:29.687 UTC
200 [ROBIN_ELVIRA_SEARCH_A1]
ROBIN_ELVIRA_SEARCH
[3/1698] ROBIN_ELVIRA_SEARCH_20170328_101729.687.IMG.gz
[80x1563]
51°56'55.4"N, 004°18'48.2"E 1299m
57.6° 5.5°
Zouteveen
Bouwlust
N468
Foppenplas
Maasland
Scoutingeiland

DEFINIÇÃO DE AREAS AUTORIZADAS E DE EXCLUSÃO



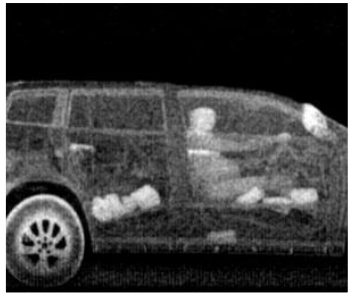
INSPEÇÃO DE PESSOAS, BAGAGENS E OUTROS ATIVOS

RX vista única

RX vista multipla

Tomografia em tempo real

Detetores de metais



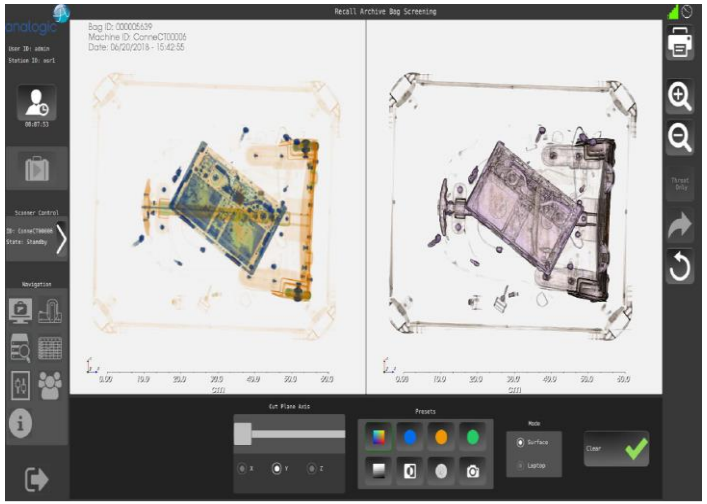
Viaturas

Deteção de radiação

Deteção de Explosivos e narcóticos

Soluções Integradas

INSPEÇÃO DE PESSOAS, BAGAGENS E OUTROS ATIVOS



CONTROLO / GESTÃO DE ACESSOS

Contextos complexos

CONTROLO / GESTÃO DE ACESSOS

- ✓ **Algumas consequências:**
  - ✓ A burocracia tende a levar à permissividade e, consequentemente, a falhas de segurança;
  - ✓ Os processos manuais são suscetíveis ao erro humano;
  - ✓ Mesmo quanto existem subsistemas de gestão de acesso, estes estão frequentemente não integrados entre eles nem com os sistemas de gestão do negócio levando à duplicação de tarefas e à probabilidade de aumento de erros;
  - ✓ A entrada de matérias primas, saídas de resíduos e de produto acabado são processos críticos de negócio cuja fluidez e correção depende de processos frequentemente suportados em contratação externa.

SISTEMAS SEGREGADOS

- Como centralizar a segurança herdando sistemas que nunca foram feitos para funcionar juntos?
- Como se garante que as operações estejam sempre em conformidade simplificando, ao mesmo tempo, os relatórios de auditoria?
- Os planos de segurança física e cibernética convergem para proteger a infraestrutura crítica das ameaças atuais e futuras?

SOLUÇÃO UNIFICADA

COMO GERIR COM EFICIÊNCIA O RISCO NAS INFRAESTRUTURAS CRITICAS?

CRIAR UMA INFRAESTRUTURA LIGADA E RESILIENTE

Alargar a segurança a todo o campus e perímetro

Contabilizar todas as pessoas em tempo real

Otimizar os relatórios de evidencias

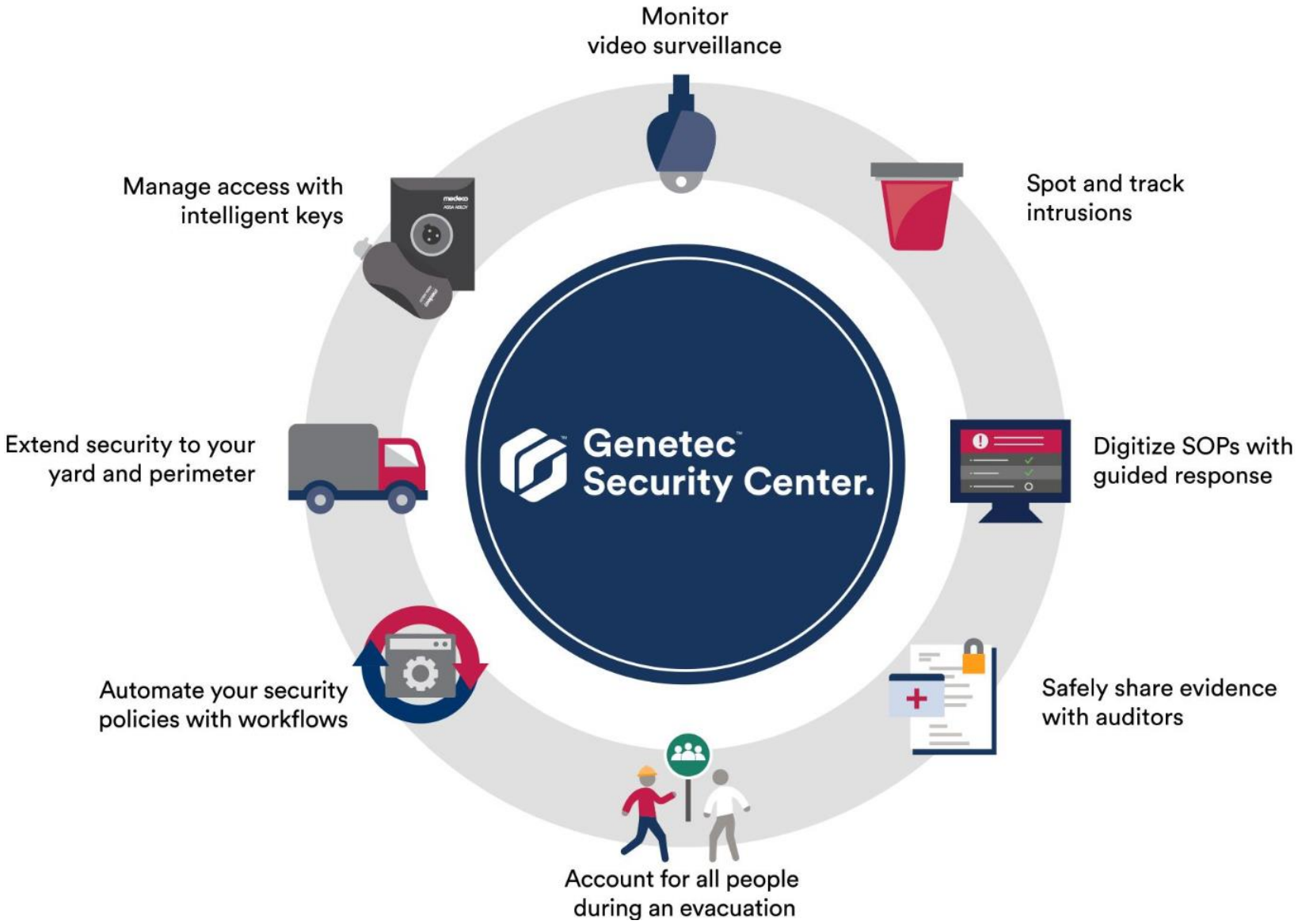
Digitalizar os procedimentos operacionais padrão

Estar ciente dos intrusos antes de violarem o perímetro

Assegurar que os subcontratados têm acesso apenas às áreas corretas

Gerir o acesso com equipamentos e sistemas em rede IP

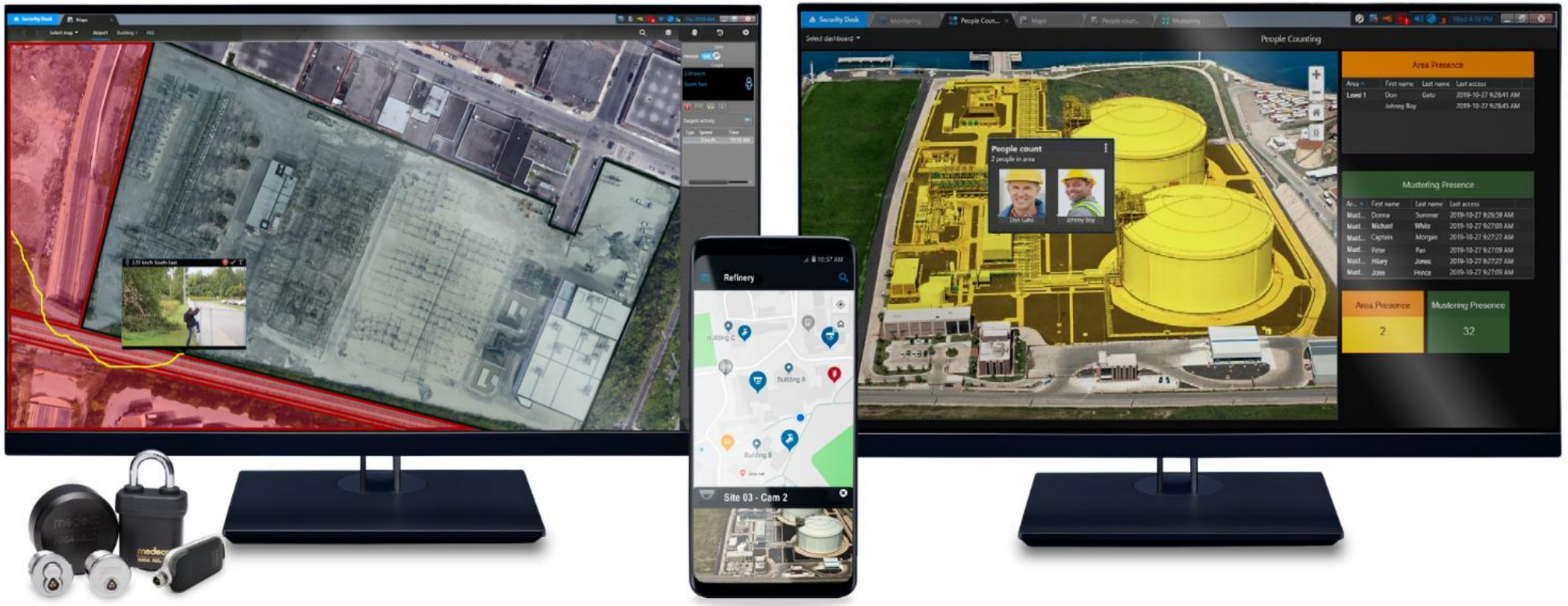
Maximizar a cobertura Video



A integração de aplicações de segurança distintas numa camada de apresentação é complexa e limitada.

É por isso que oferecemos um portfólio de soluções de segurança unificadas criadas e projetadas de origem tendo em mente as infraestruturas críticas

PRINCIPAIS COMPONENTES

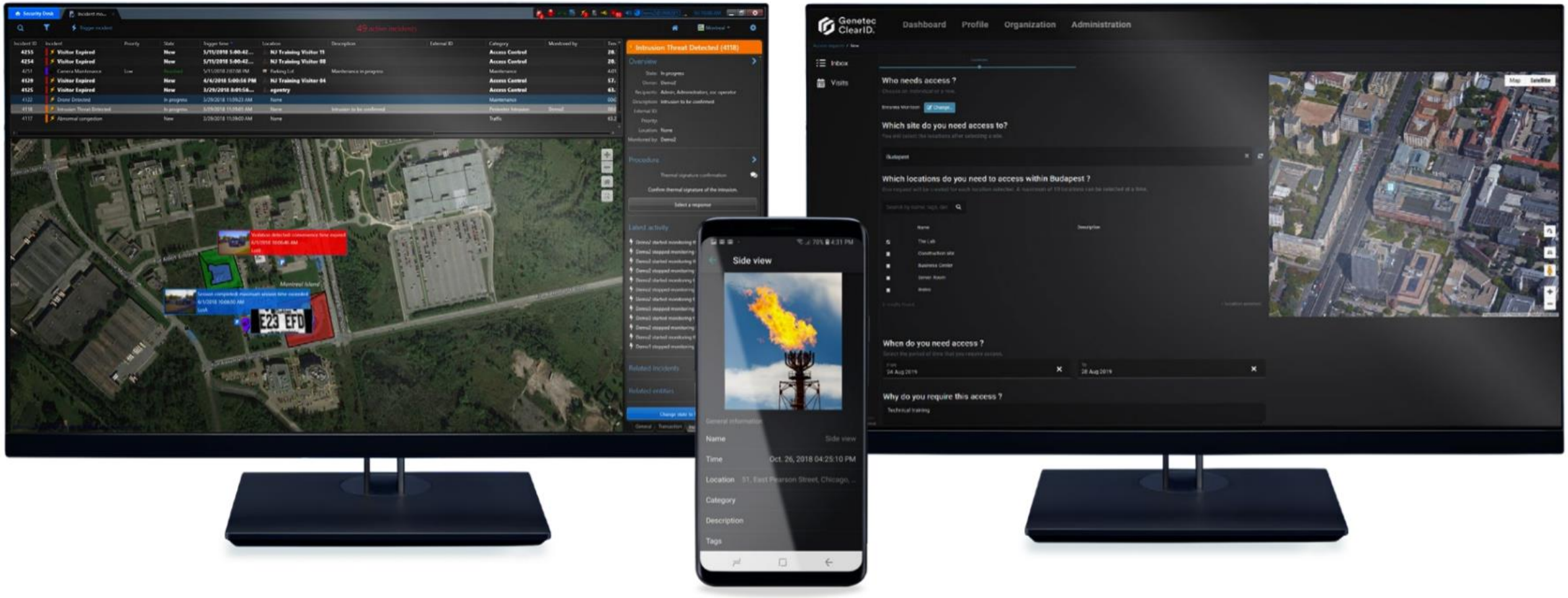


Intrusion and restricted security area

Intelligent key management

Muster and accountability reports

PRINCIPAIS COMPONENTES



Genetec Mission Control.

Genetec Clearance.

Genetec ClearID.

PRINCIPAIS FUNCIONALIDADES

Gestão por níveis de ameaças

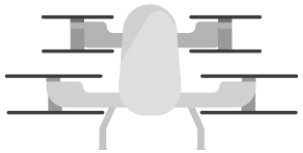
Videovigilância e monitorização da sua integridade

Integração com SCADA

Mobilidade

Tracking Visual

Reporting Visual



Integração com Drones

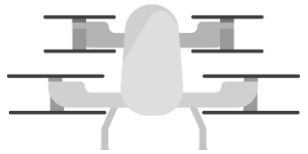
Alta disponibilidade e disaster recovery

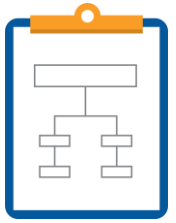
Multiplas opções de deployment

Segurança e privacidade total

EXEMPLOS: INTRUSÃO

1.	2.	3.	4.	5.	6.
Deteção de intrusões não autorizadas no perímetro	Induzir intrusos a abandonar a área	Tomar medidas de segurança para atrasar o acesso do intruso	Avaliar a legitimidade de um incidente de intrusão	Comunicar as invasões detetadas com a força de trabalho	Tome medidas imediatas para deter o intruso
Detetar	Avisar	Atrasar	Averiguar	Comunicar	Responder





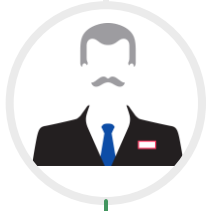
EXEMPLOS: SUBCONTRATADOS

Ana trabalha para uma concessionária IC e precisa emitir uma ordem de serviço para reparar uma bomba de óleo

José trabalha para uma grande empresa de engenharia e gere o trabalho do empreiteiro

Ela cria uma ordem de serviço e define as especificações do trabalho

A ordem de serviço é enviada para a empresa de engenharia

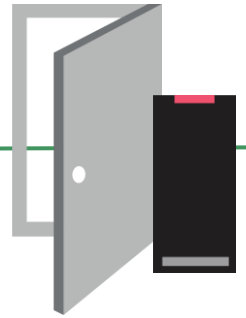


Ele associa empreiteiros para responder às necessidades do trabalho

* Os perfis do contratante são enviados para ClearID

o novo perfil do titular do cartão é criado automaticamente e recebe o acesso apropriado

A ClearID fornece o acesso do contratante no Synergis

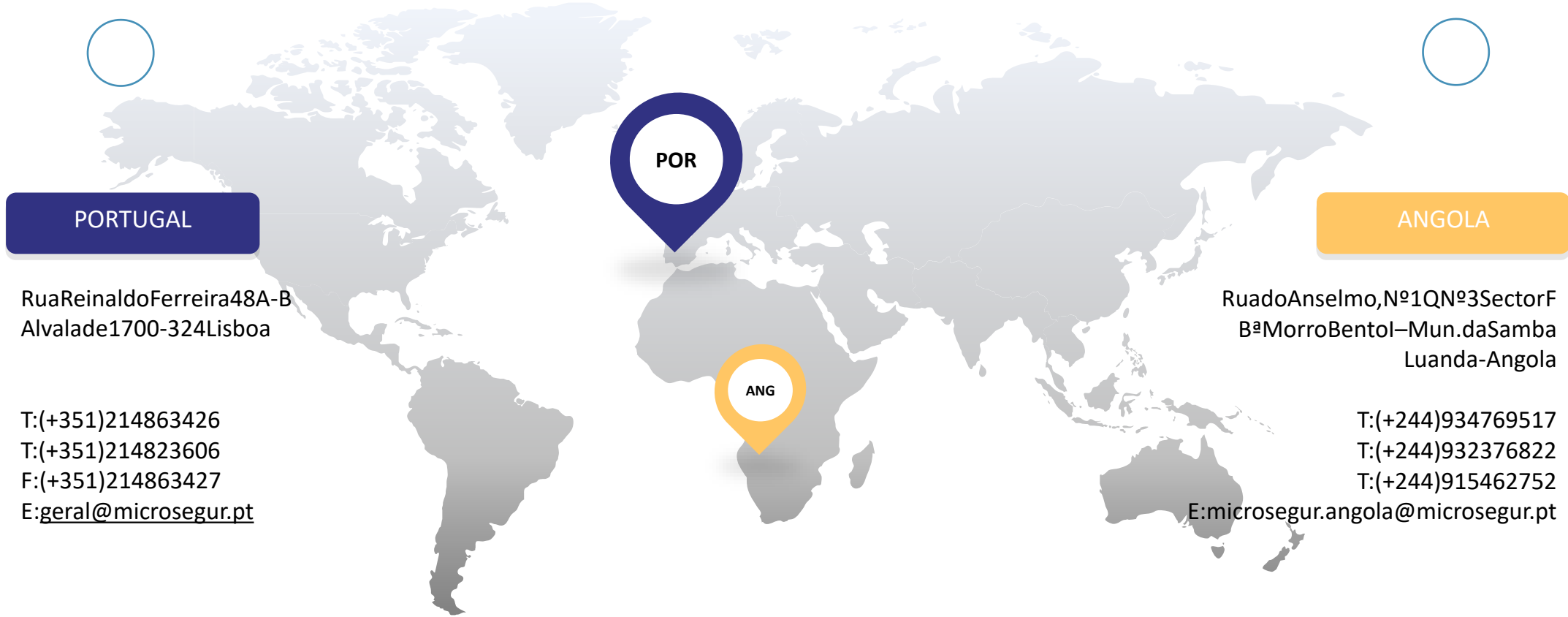


Empreiteiros fazem check-in e podem começar a trabalhar

* Roadmap item

GESTÃO DA INFORMAÇÃO

Obrigado!



PORTUGAL

RuaReinaldoFerreira48A-B
Alvalade1700-324Lisboa

T:(+351)214863426
T:(+351)214823606
F:(+351)214863427
E:geral@microsegur.pt

ANGOLA

RuadoAnselmo,Nº1QNº3SectorF
BªMorroBentoI–Mun.daSamba
Luanda-Angola

T:(+244)934769517
T:(+244)932376822
T:(+244)915462752
E:microsegur.angola@microsegur.pt

MICROSEGUR
Soluções integradas de tecnologia e segurança

www.microsegur.pt