Govern d'Andorra

ANDORRA DIGITAL

ANC AD

2ª Jornada CISO

Desvetllant els Secrets del Cel Digital: Ciberseguretat al Cloud i Protecció de Dades

David de Nadal

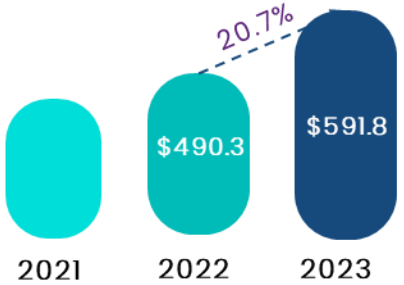
1 de Març de 2024

L'adopció del núvol no s'atura...

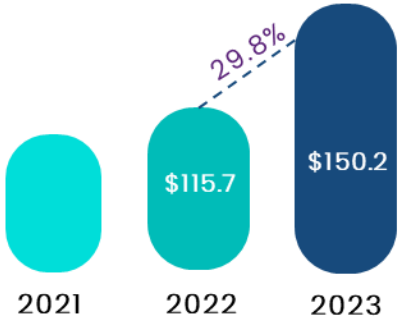
El Cloud Computing s'ha establert com la nova normalitat per a les TI empresarials

Model de responsabilitat compartida

Es preveu que la despesa mundial dels usuaris finals en serveis al núvol públic creixi un 20,7% fins a un total de 591.800 milions de dòlars el 2023, més que els 490.300 milions de dòlars el 2022.



Es preveu que la infraestructura com a servei (IaaS) experimenti el major creixement de la despesa dels usuaris finals el 2023, amb un 29,8%



Gartner Forecasts Worldwide Public Cloud End-User Spending to Reach Nearly $600 Billion in 2023

...estem més segurs? Sí... però...

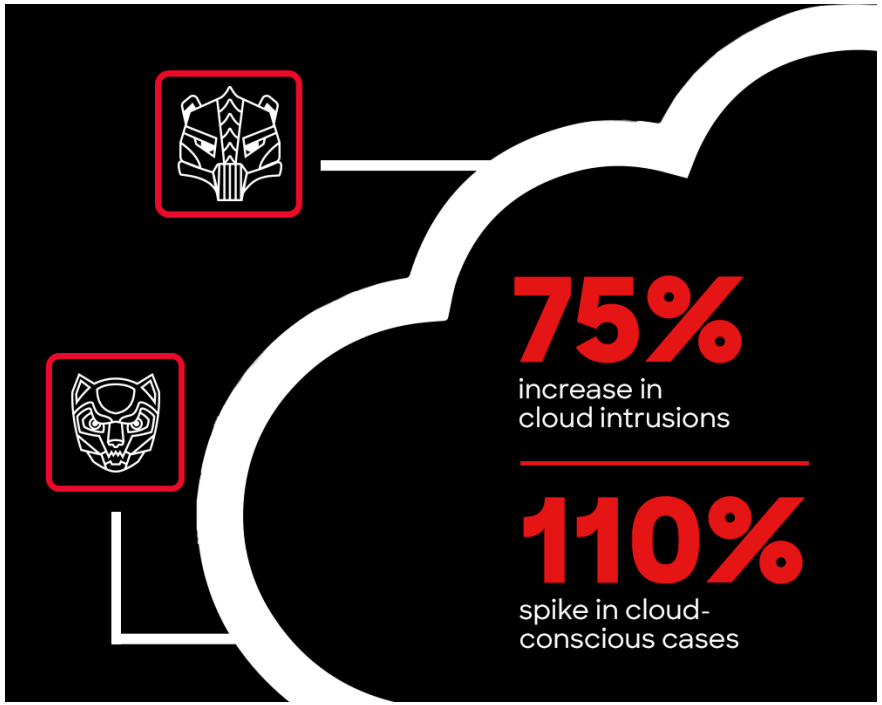
Model de responsabilitat compartida

Gairebé el **100%** de les explotacions relacionals es van originar en proveïdors comercials de programari

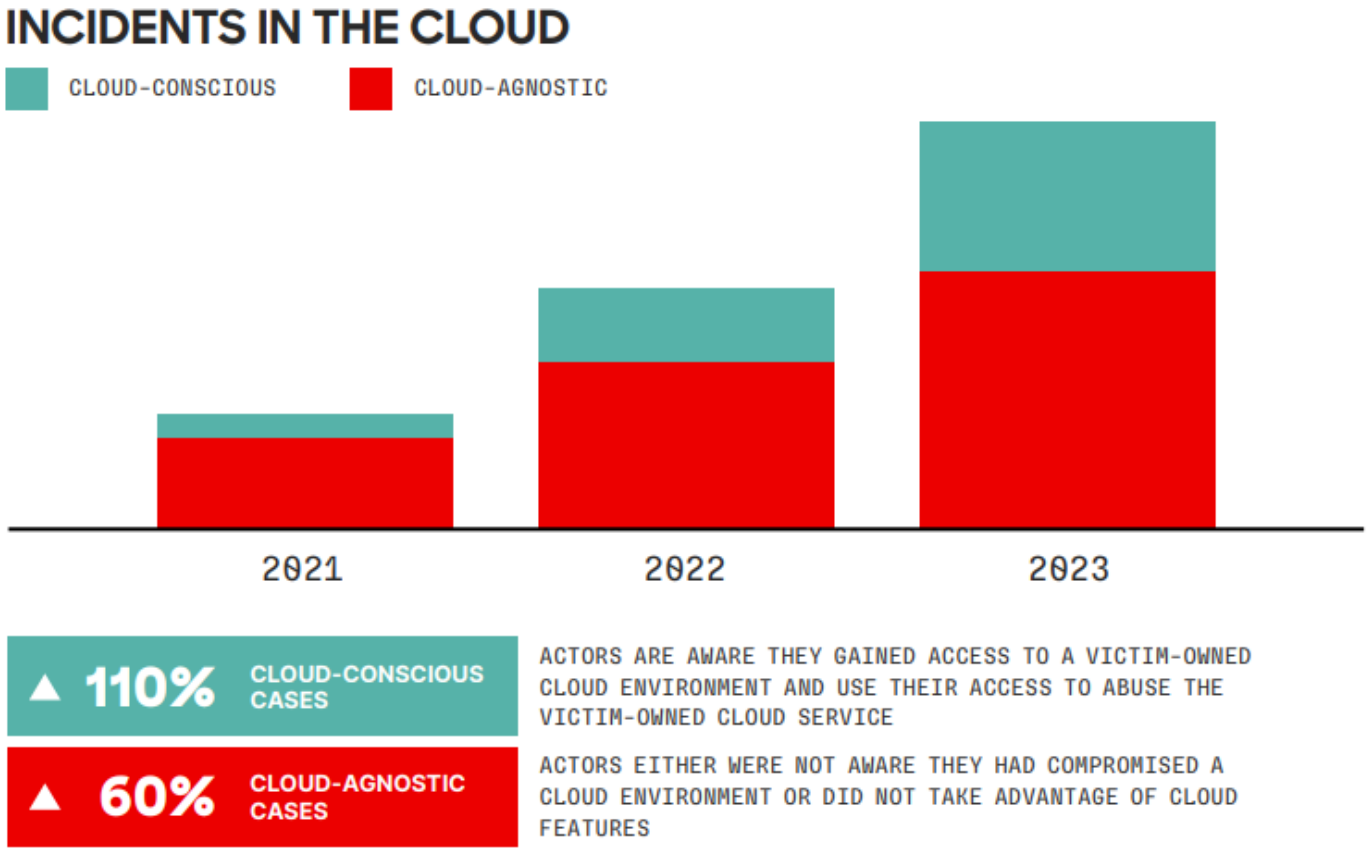
...estem més segurs?

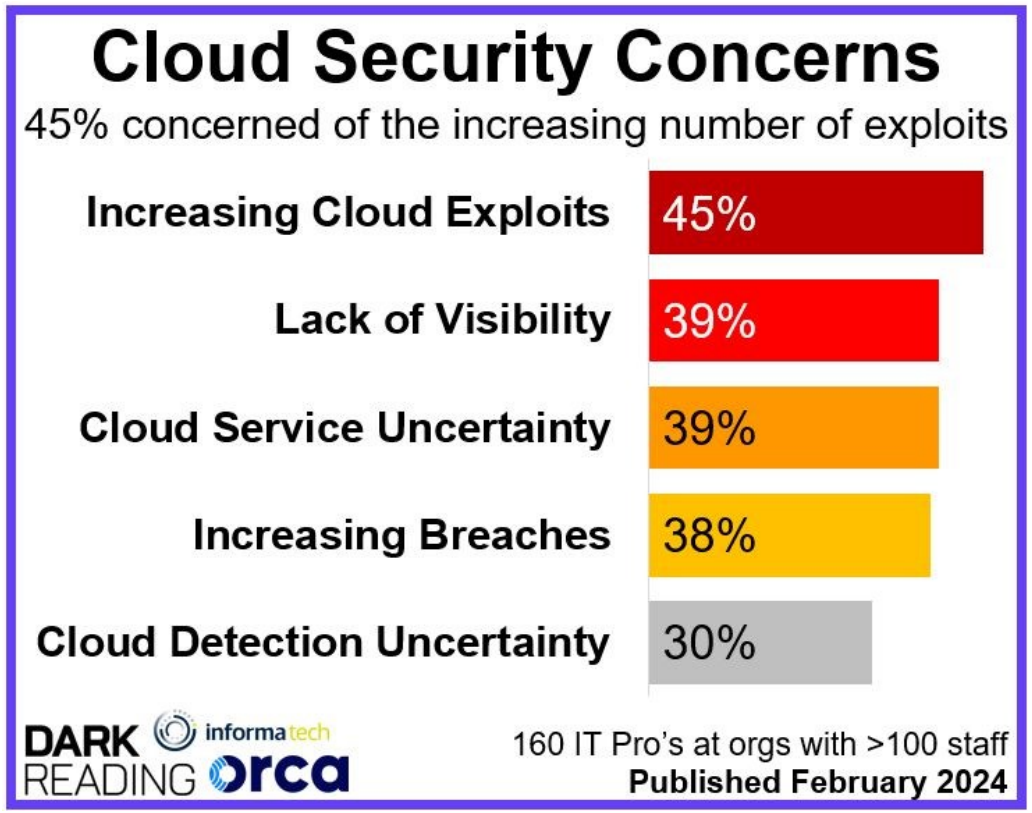
Els adversaris dominen el núvol

Els adversaris estan aprofitant l'adopció global del núvol, fent del núvol un camp de batalla principal. Els adversaris conscients del núvol, especialment els actors d'eCrime, utilitzen credencials vàlides per accedir als entorns de núvol de les víctimes i, a continuació, utilitzen eines legítimes per executar el seu atac, cosa que dificulta la distinció entre l'activitat normal de l'usuari i una violació.



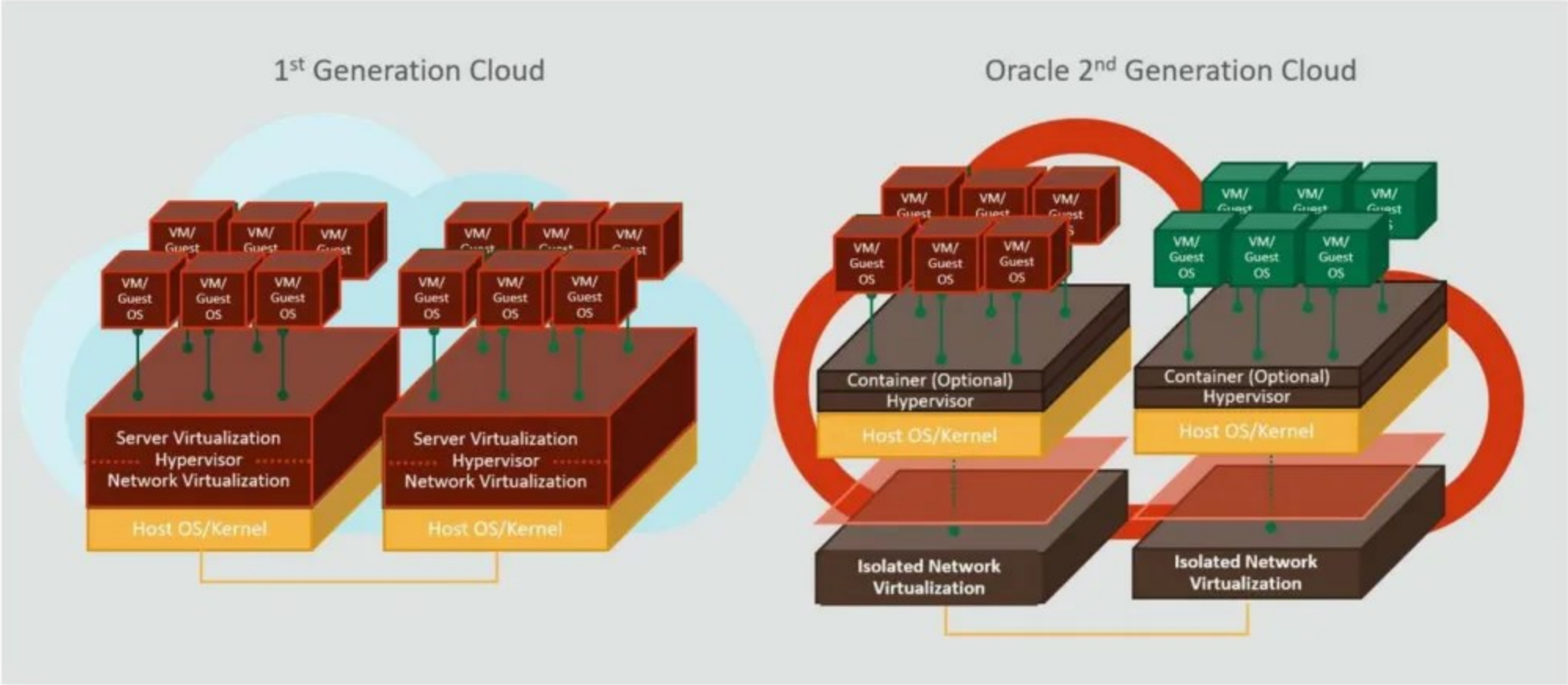
...estem més segurs?





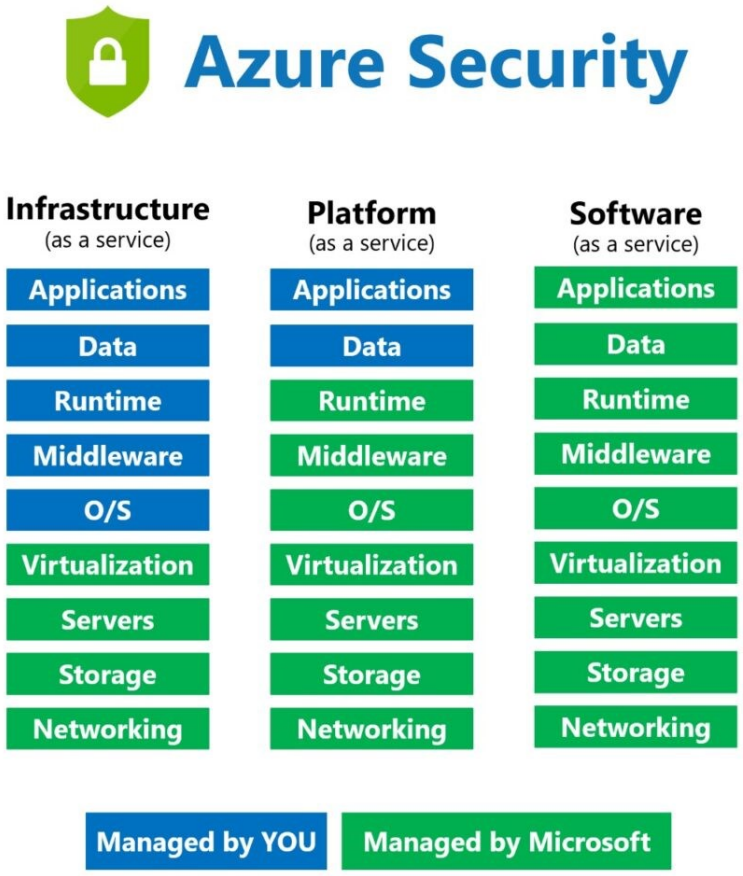
...estem més segurs?

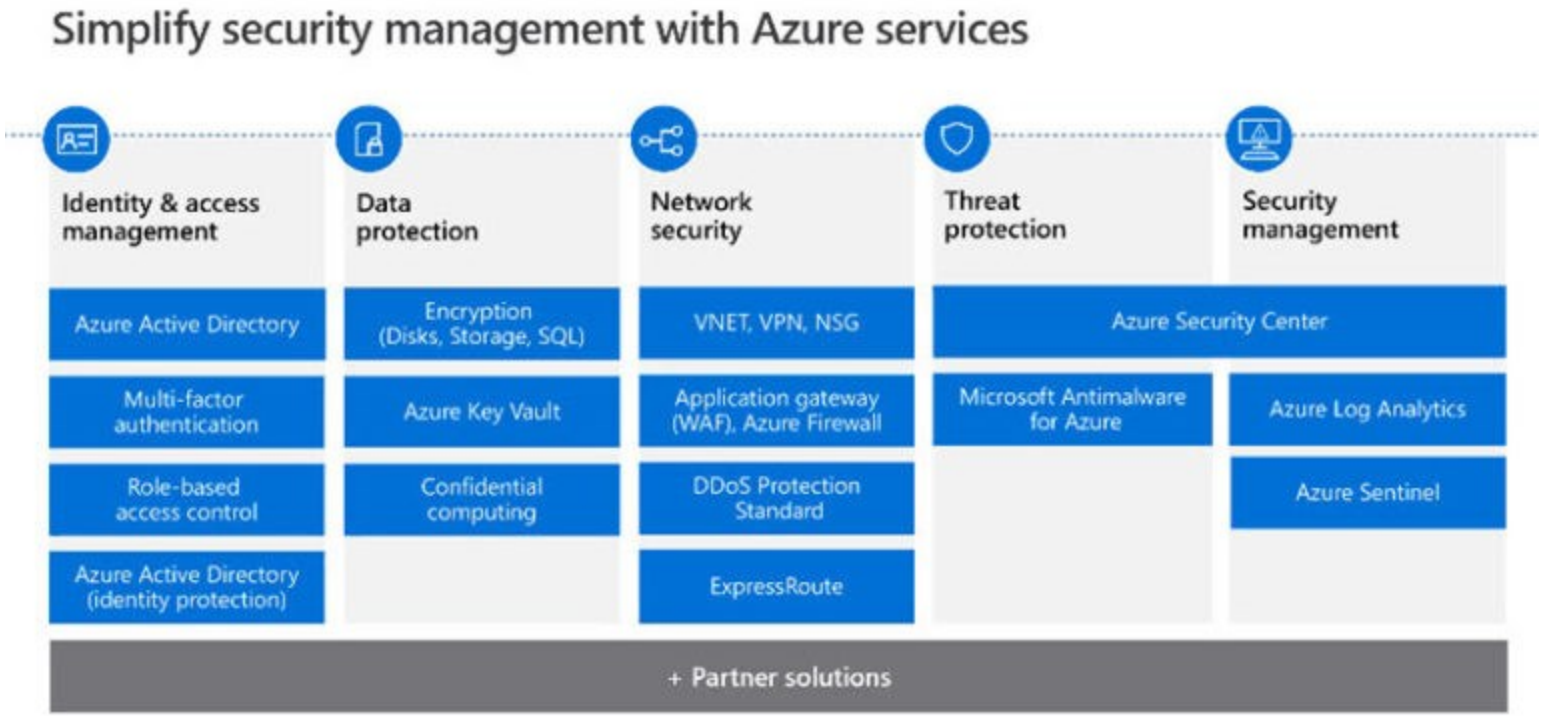
Exemple de millores del proveïdors de Cloud



...estem més segurs?

Exemple de millores del proveïdors de Cloud





Per què ens passa això?

> La configuració de Google Groups mal configurada de les organitzacions filtra dades de credencials

> Dades sobre 123 milions de llars dels Estats Units exposades a causa d'un Bucket d'AWS S3 mal configurat

> Sistemes d'orquestració de contenidors exposats que posen en risc moltes organitzacions

Per on comencem a posar fil a l'agulla?

Cas Prosegur

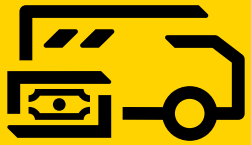
1. MFA i Centralitzar la visibilitat dels entorns privats, híbrids i multinúvol.
2. Utilitzeu un tallafoc d'aplicacions web per protegir les vostres aplicacions natives del núvol.
3. Implementant un automatisme de cerca d'amenaces que s'actualitzi dinàmicament i de forma continua
4. Utilitzeu capacitats d'intel·ligència d'amenaces per anticipar-se a les properes amenaces i prioritzar de manera eficaç per prevenir-les

Per on comencem a posar fil a l'agulla?

Cas Prosegur

PROSEGUR SECURITY

- 14 països
- +100.000 guardes de seguretat
- 25 centres de control



PROSEGUR CASH

- 20 països
- +10.000 v ehicles en flota
- +100.000 ATM gestionats

PROSEGUR ALARMS

- 9 països
- +604.000 alarmes connectades
- +18.000 v ehicles i dispositius geolocalitzats

CIPHER

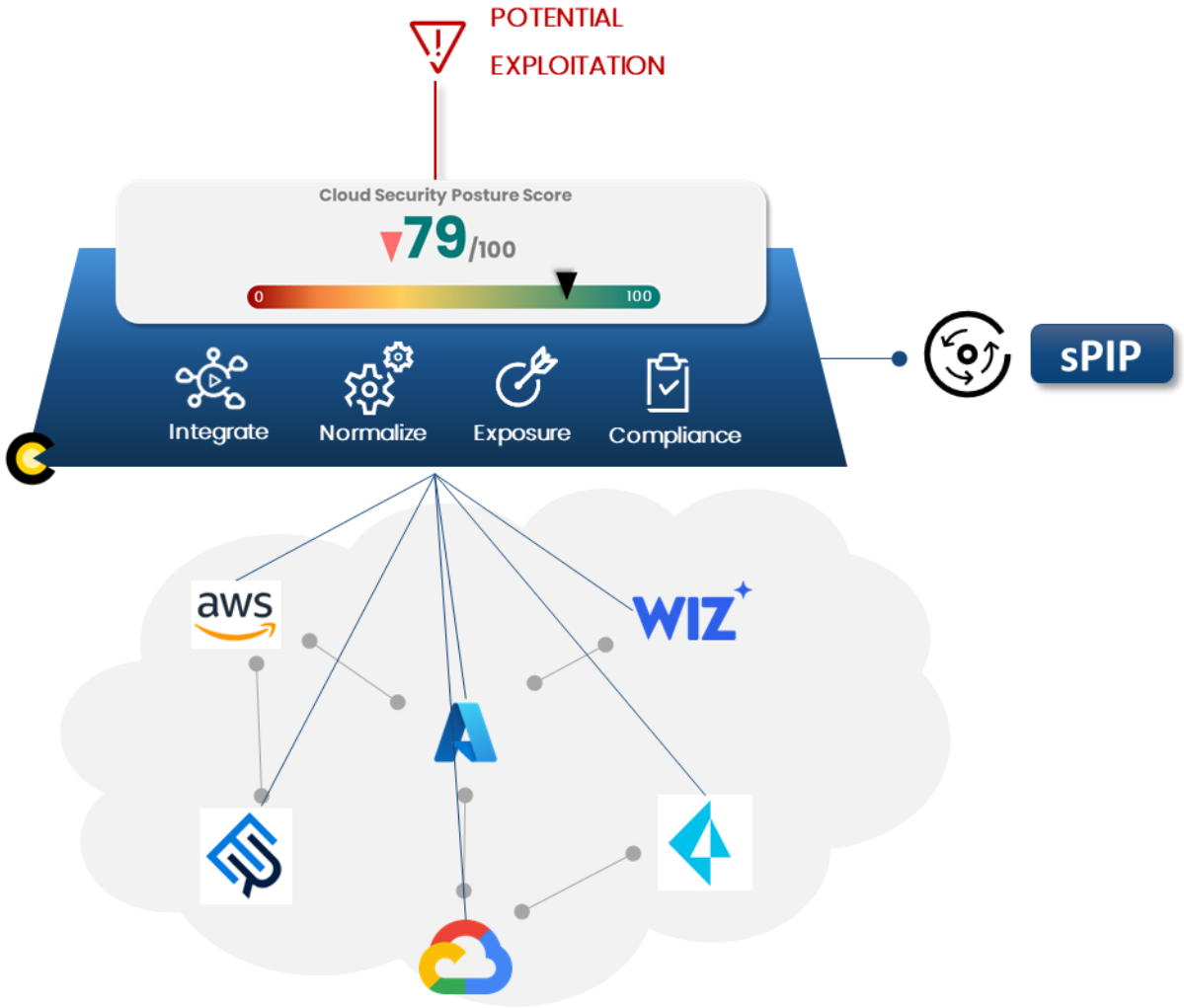
- +18 països
- +400 Ciber-experts
- 6 SOCs al món
- +150 TB analitzats per dia
- +1000 clients

PROSEGUR AVOS

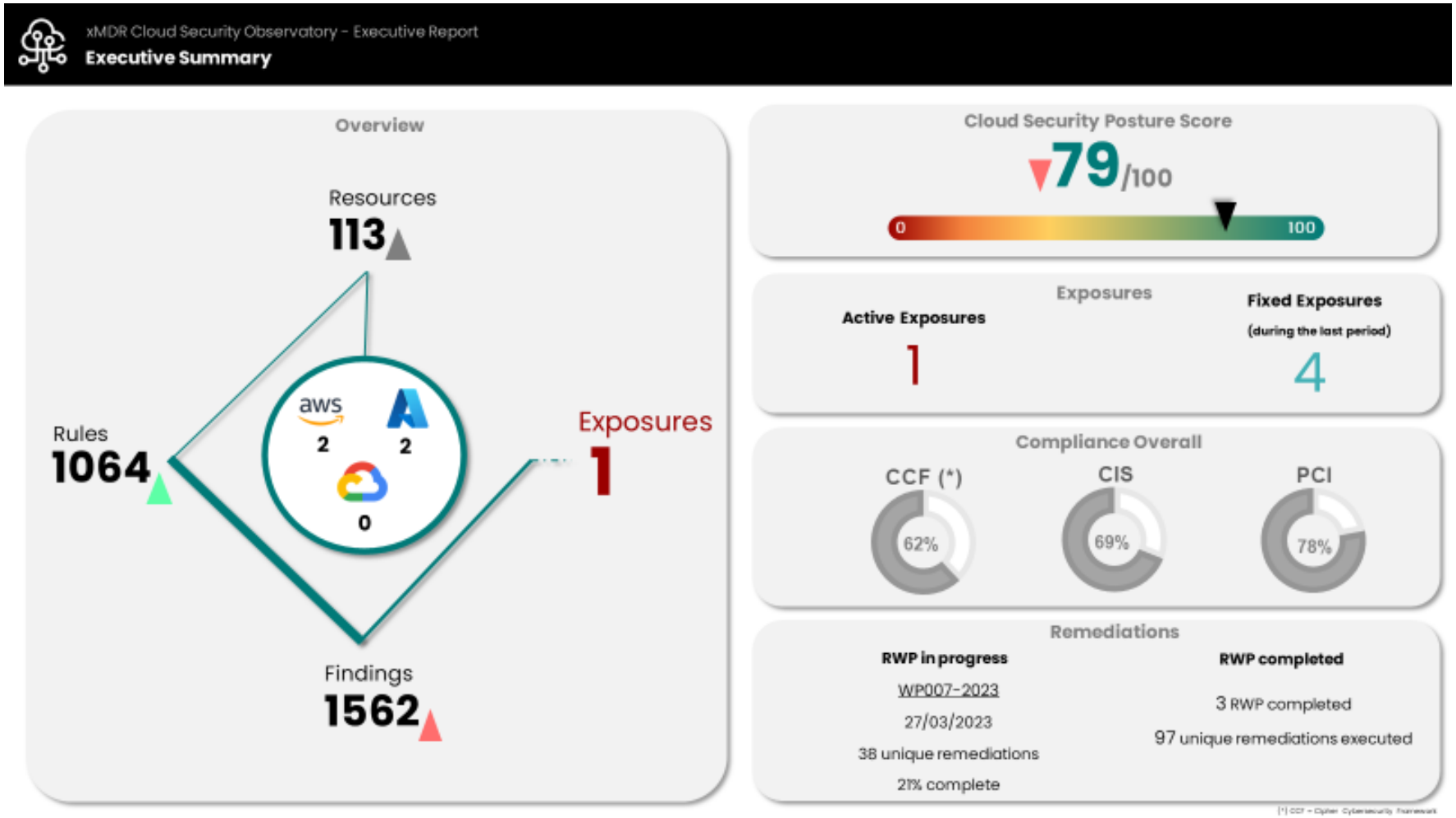
- 1 país
- Experts en Transformació Digital
- Experts en sector financier

Centralitzar la visibilitat dels entorns privats, híbrids i multinúvol.

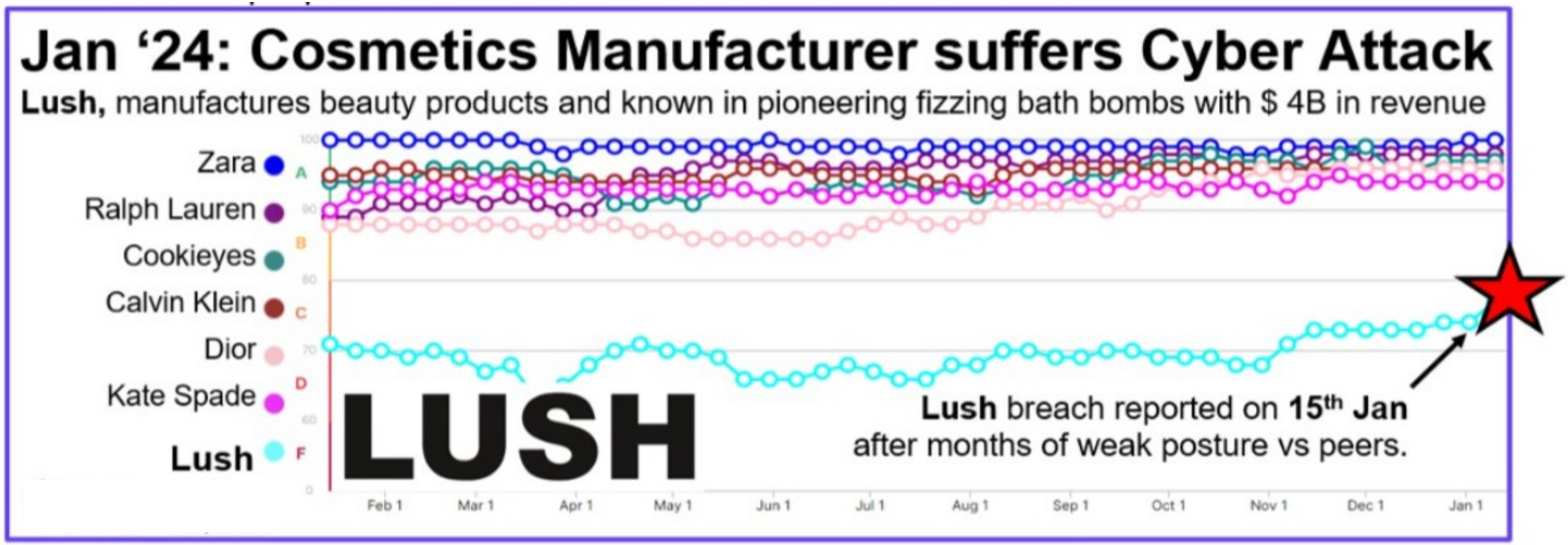
Disposar d'una puntuació de seguretat unificada en el núvol i caçar explotacions potencials per identificar aquelles debilitats que podrien suposar un compromís immediat per al negoci.



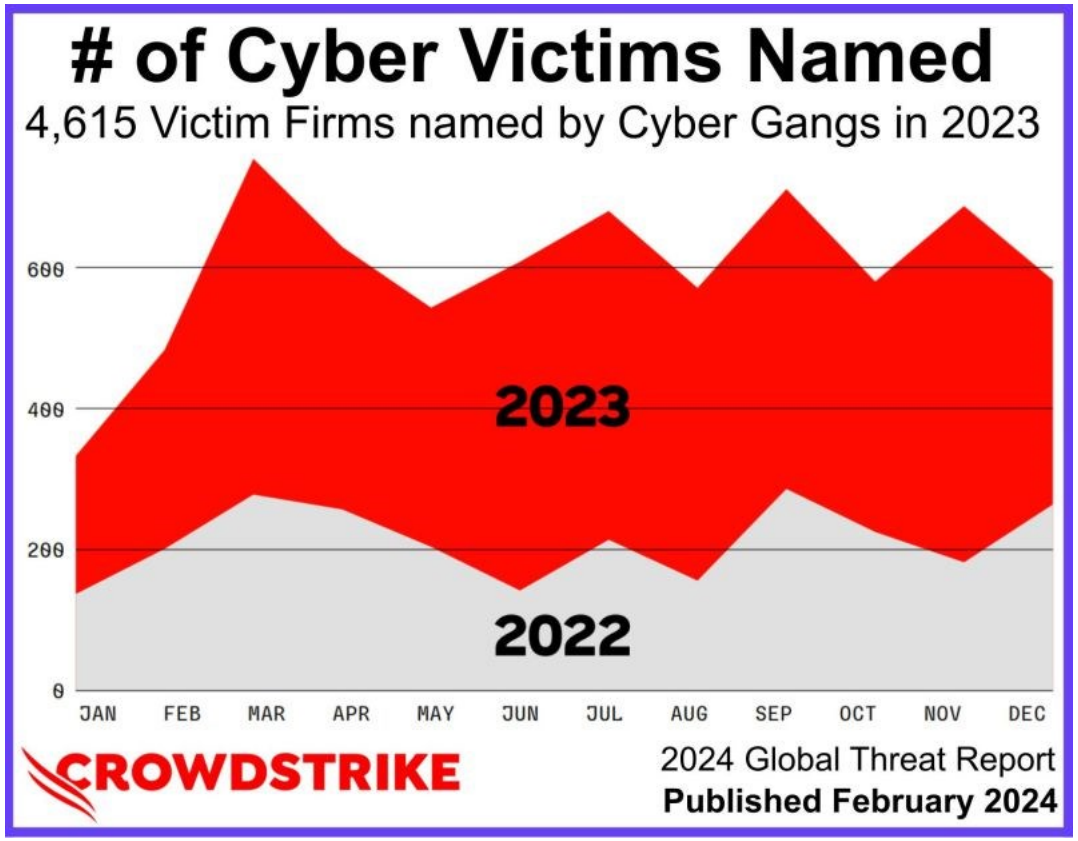
Centralitzar la visibilitat dels entorns privats, híbrids i multinúvol.



Centralitzar la visibilitat dels entorns privats, híbrids i multinúvol.



El bon scoring - Normativa, compliment i sancions



Endesa: multa històrica de 6.100.000 euros per violació greu de protecció de dades

Segons l'informe de l'AEPD, les dades personals de 4,8 milions de clients d'electricitat i 1,2 milions de gas d'Endesa van estar exposades a tercers no autoritzats.

A més, es va identificar la possibilitat d'accedir a dades tècniques de 30,6 milions de punts de subministrament elèctric i 8,6 milions de gas, incloent-hi informació confidencial com noms, cognoms, DNI, telèfons, correus electrònics, adreces postals, números de compte bancària, CUPS (punt de subministrament), consum, facturació i deutes.

El bon scoring - Normativa, cumpliment i sancions

AIXÍ ES DESGLOSA LA SANCIÓ CONTRA ENDESA

La sanció imposada per l'AEPD es desglossa en diverses infraccions del Reglament General de Protecció de Dades (RGPD):

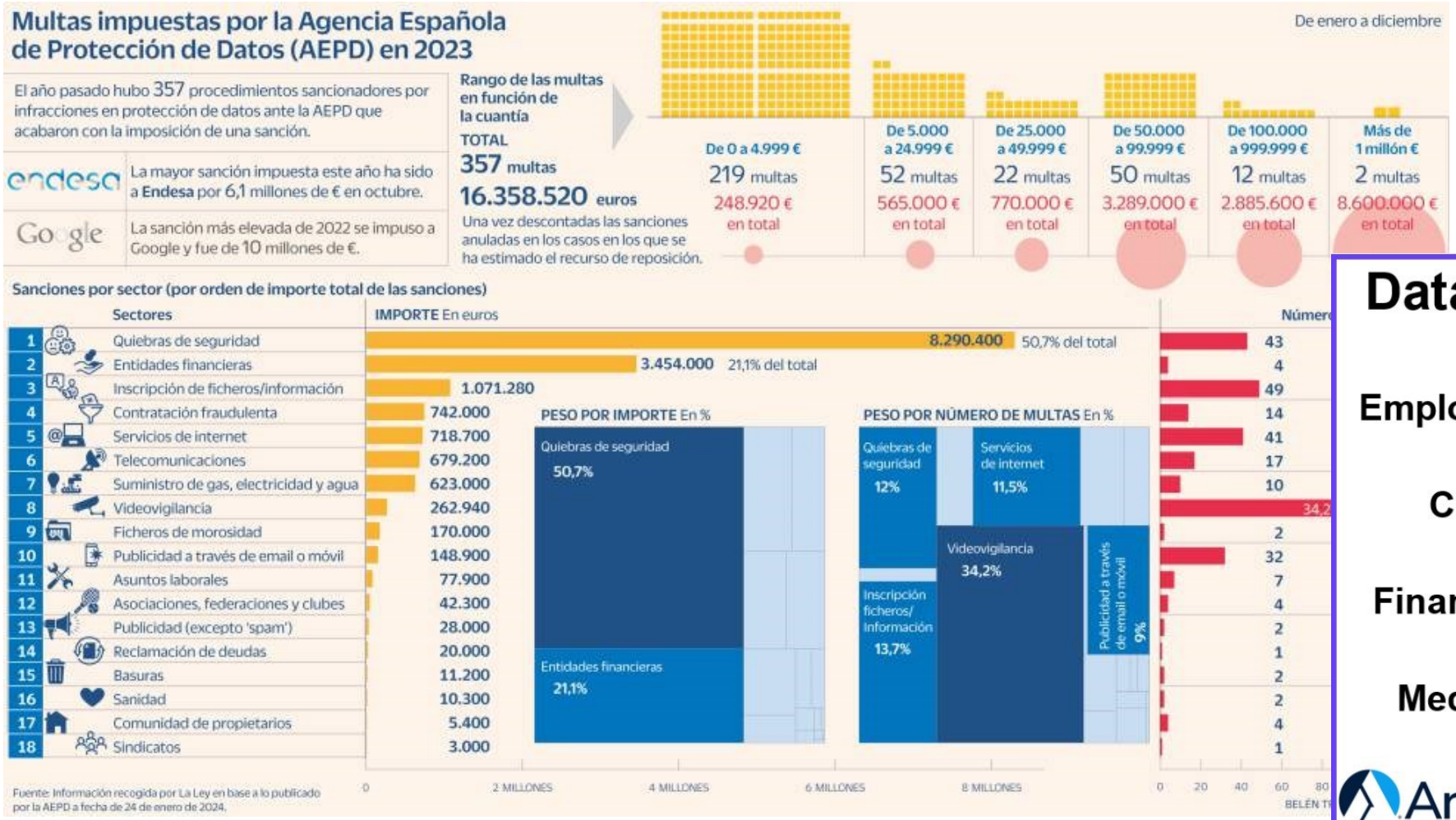
- Infracció de l'article 5.1.f) de l'RGPD: multa de 2.500.000 euros..
- Infracció de larticle 32 del RGPD: Multa de 1.500.000 euros..
- Infracció de l'article 33 del RGPD: multa de 800.000 euros.
- Infracció de l'article 34 del RGPD: multa de 800.000 euros.
- Infracció de l'article 44 del RGPD: multa de 500.000 euros.

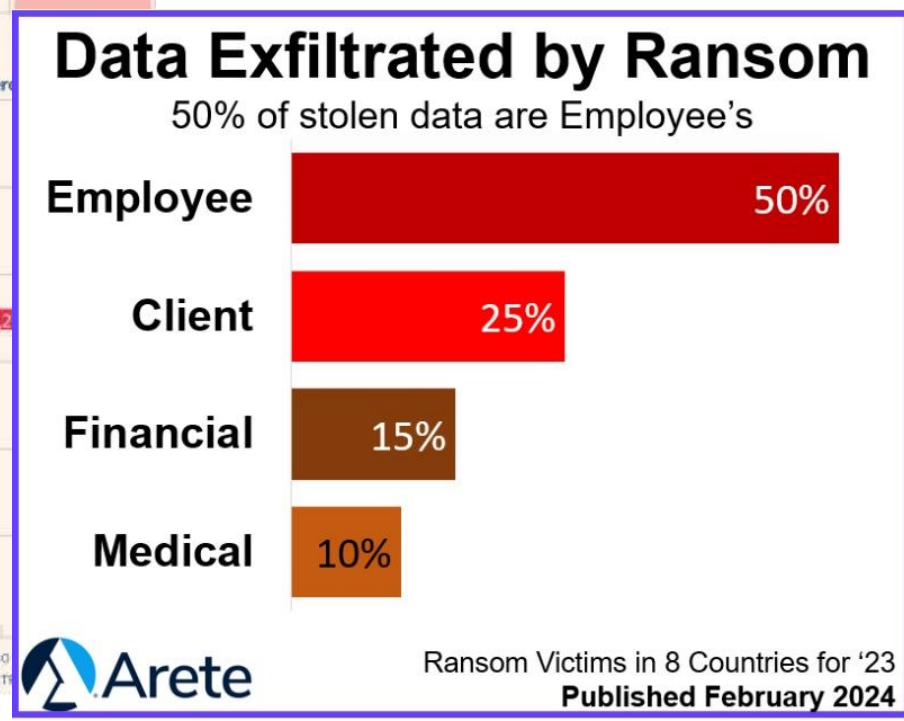
Endesa: multa històrica de 6.100.000 euros per violació greu de protecció de dades

Segons l'informe de l'AEPD, les dades personals de 4,8 milions de clients d'electricitat i 1,2 milions de gas d'Endesa van estar exposades a tercers no autoritzats.

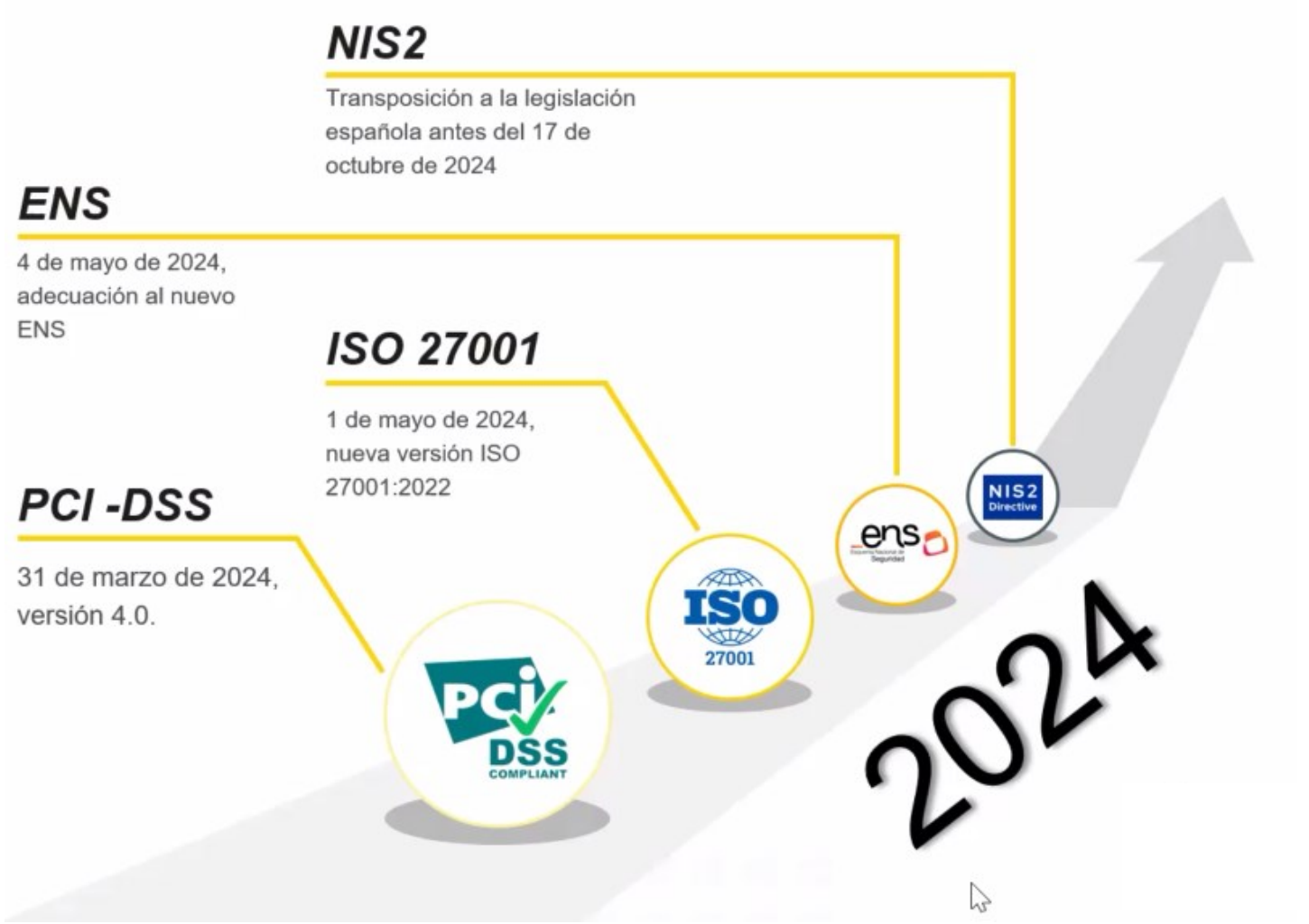
A més, es va identificar la possibilitat d'accedir a dades tècniques de 30,6 milions de punts de subministrament elèctric i 8,6 milions de gas, incloent-hi informació confidencial com noms, cognoms, DNI, telèfons, correus electrònics, adreces postals, números de compte bancària, CUPS (punt de subministrament), consum, facturació i deutes.

El bon scoring - Normativa, cumpliment i sancions





El bon scoring - Normativa, cumpliment i sancions



El bon scoring - Normativa, compliment i sancions

Sectors d'alta criticitat

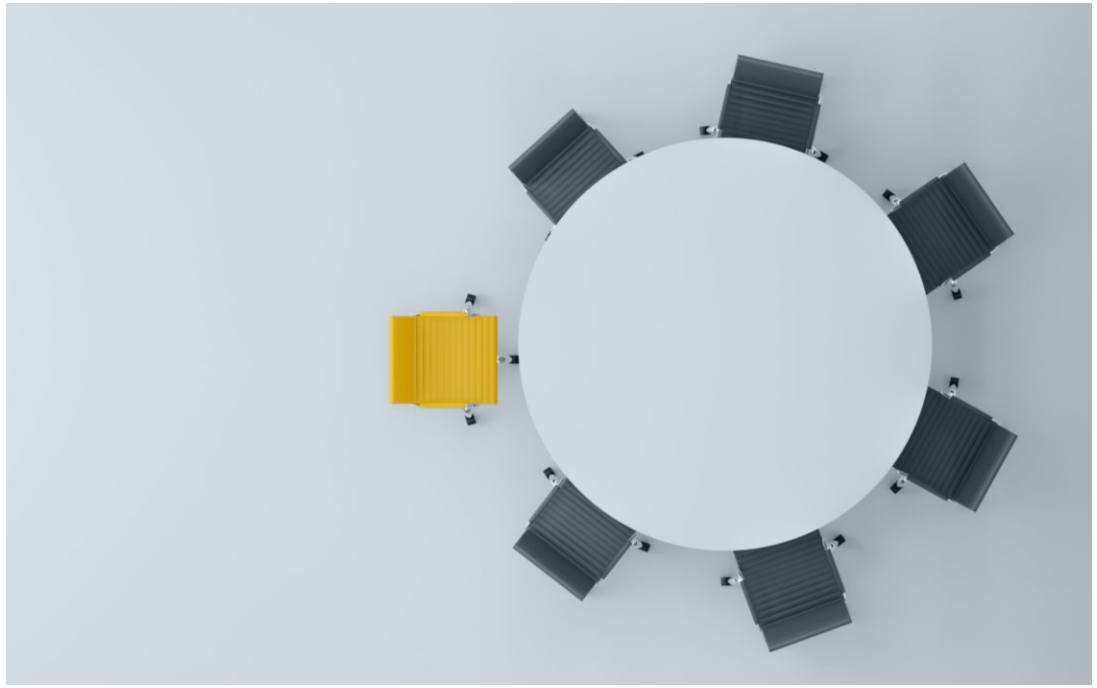
- Energia
- Transport
- Banca
- Sector sanitari
- Aigües residuals
- Espai
- GAS
- Infraestructures dels mercats financers
- Administració pública
- Aigua potable
- Infraestructura digital
- Gestió de serveis TIC

El bon scoring - Normativa, compliment i sancions

Una de les principals novetats és la responsabilitat legal en cas de un ciberatac...

Equip directiu

S'exigirà que activitats de **prevenció** i **resposta a incidents** funcionin de forma **eficaç**, és a dir, d'una forma proactiva i no merament reactiva.



Pagament de **sancions** que podran arribar a suposar **10M€ o el 2% de la facturació** anual, o fins i tot la **prohibició d'exercir** càrrecs relacionats amb la gestió empresarial.

El bon scoring - Normativa, cumpliment i sancions

Las principales obligaciones recogidas en la Directiva NIS2

- Desenvolupar **polítiques i procediments per avaluar l'eficiència** de la gestió de riscos de ciberseguretat.
- Establir **controls** de supervisió sobre l'**adquisició de tecnologies i serveis.**
- Comptar amb solucions d'**autenticació multifactor, comunicacions i sistemes segurs** per les comunicacions d'emergència.
- Prestar la diligència deguda en **supervisar la cadena de suministrament,** la relació entitat-proveïdor amb el cumpliment de las mesures de ciberseguretat.
- Vetllar per la **seguretat de les persones**, el control d'acceso i la gestió d'actius.
- Tenir definit **un protocol d'actuación d'incidents** de seguretat que **garantitzi** el cumpliment de **notificació obligatòria** a les autoritats dins dels plaços previstos, fins i tot **de potencials bretxes**.
- Disposar de **plans de continuitat** de les activitats de la organització.
- **Formar a tots els empleats** i, concretament, a **la alta direcció** en matèria de ciberseguretat.
- Realitzar una serie de mesures de prevenció que incloguin **la realització de simulacres i** proves que permetin posar en pràctica els processos establerts i verificar l'eficàcia en la resposta.

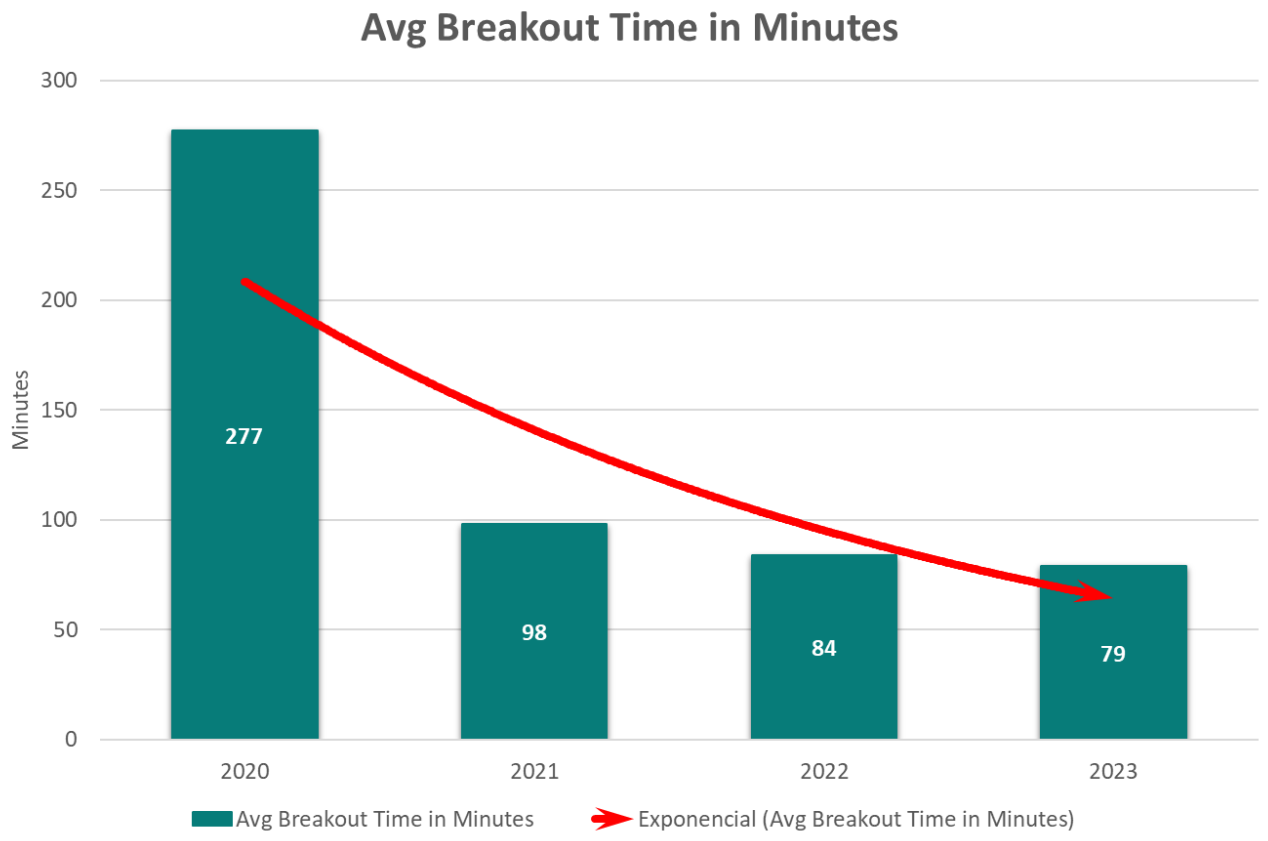
Per on comencem a posar fil a l'agulla?

Cas Prosegur

1. MFA i Centralitzar la visibilitat dels entorns privats, híbrids i multinúvol.
2. Utilitzeu un tallafoc d'aplicacions web per protegir les vostres aplicacions natives del núvol.
3. Implementant un automatisme de cerca d'amenaces que s'actualitzi dinàmicament i de forma continua
4. Utilitzeu capacitats d'intel·ligència d'amenaces per anticipar-se a les properes amenaces i prioritzar de manera eficaç per prevenir-les

Automatisme de cerca d'amenaces

Atacs més rapids – punt de saturació?



MALWARE-FREE ACTIVITY

»

75% 2023

71% 2022

62% 2021

51% 2020

40% 2019

Govern d'Andorra

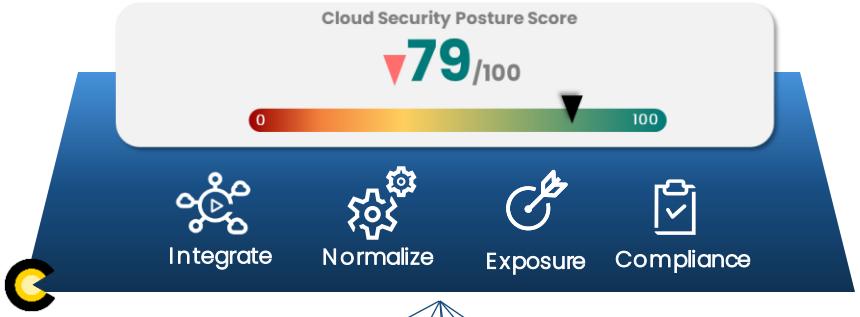
ANDORRA DIGITAL

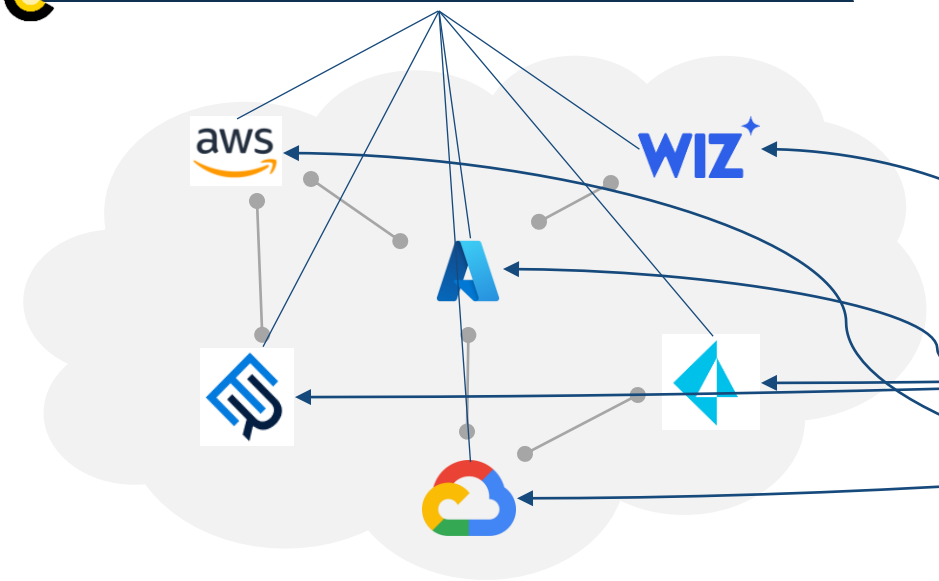
ANC-AD

Automatisme de cerca d'amenaces

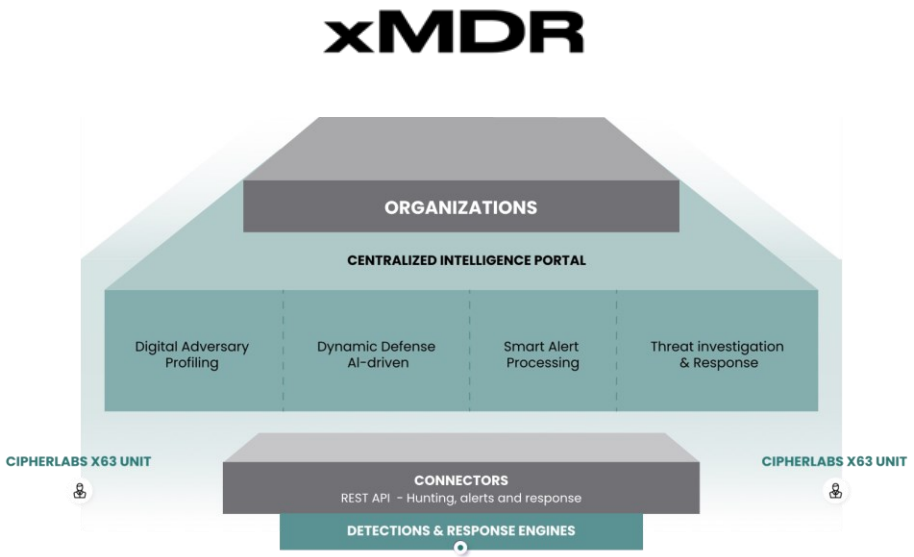
Cas Prosegur

Postura de seguretat





Visibilitat, detecció i resposta d'amenaces amb IA



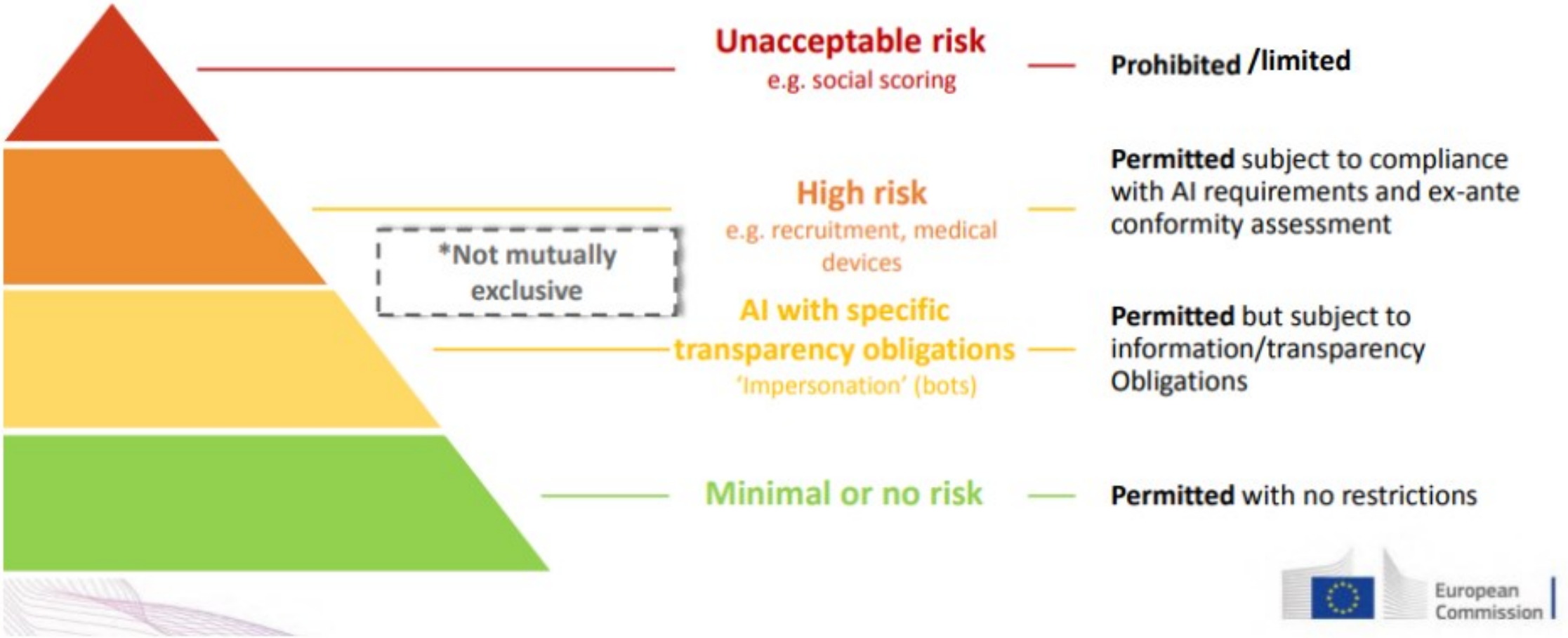
Govern d'Andorra

ANDORRA DIGITAL

ANC-AD

Ampliem l'ús Ide la IA a l'empresa – val per tot?

AIA, por Artificial Intelligence Act – Reglament Europeu sobre IA



Ampliem l'ús Ide la IA a l'empresa – val per tot?

AIA, por Artificial Intelligence Act – Reglament Europeu sobre IA

SANIDAD

La IA llama a la consulta del médico

V+

• La Generalitat planea implantar una herramienta que transcribe la conversación facultativo-paciente y rellena la historia clínica

Un médico atiende a una paciente en el CAP La Marina, en Barcelona (Mané Espinosa/ARCHIVO)

ANTONI LÓPEZ TOVAR
BARCELONA
26/02/2024 00:05 | Actualizado a 26/02/2024 08:26

Guanyarem **3 minuts** per visita médica…

… com es mantindrà el nivel de seguretat i confidencialitat de les dades dels pacients?

Ampliem l'ús Ide la IA a l'empresa

SaaS i filtració de dades a les IA

Govern d'Andorra

ANDORRA DIGITAL

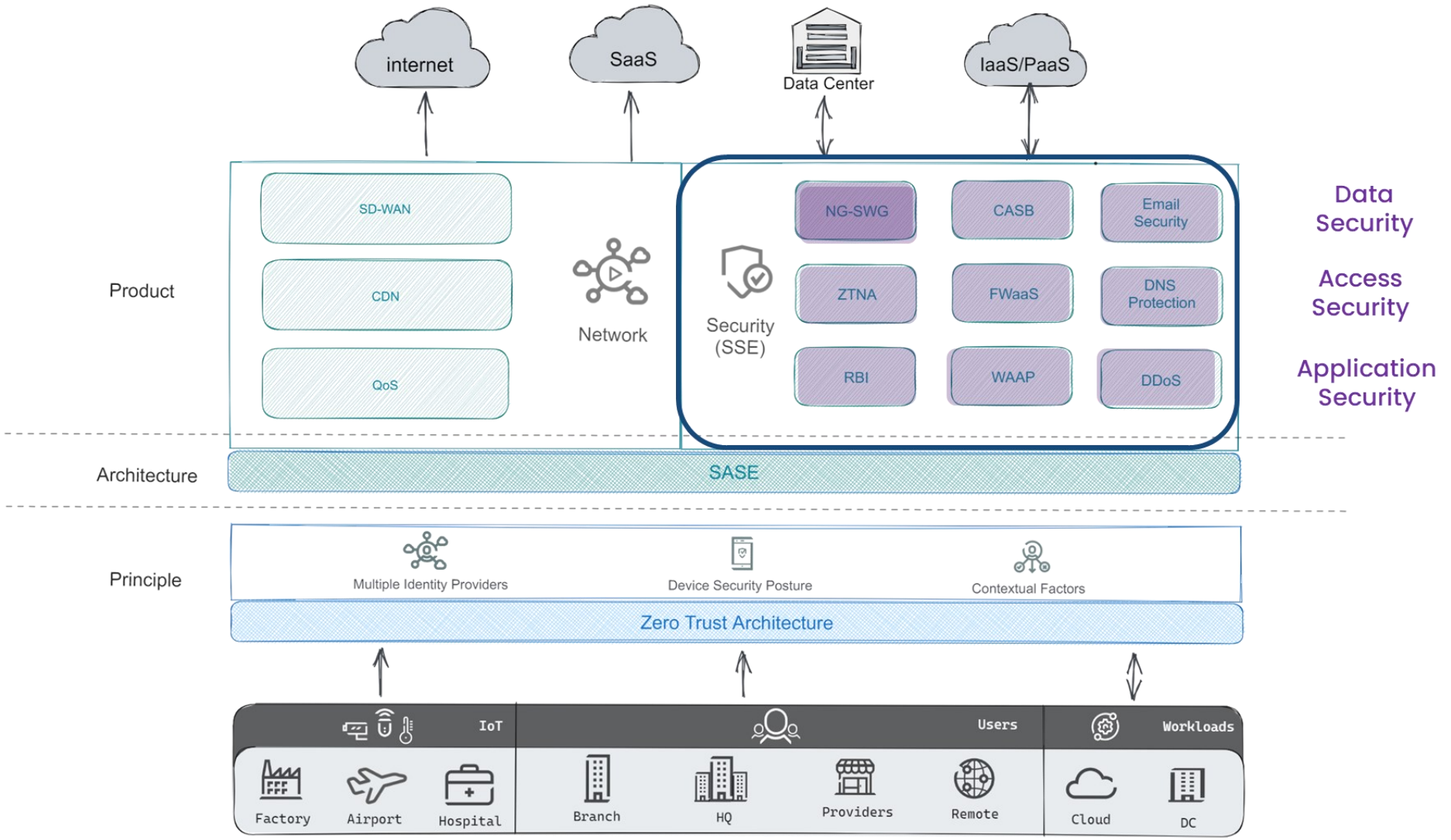
ANC-AD

Següents passes

Cas Prosegur

1 Utilitzeu capacitats d'intel·ligència d'amenaces per anticipar-se a les properes amenaces i prioritzar de manera eficaç per prevenir-les

2 Adoptar la confiança zero autoritzant l'accés només als usuaris que realment ho necessiten i només als recursos que necessiten.



Conclusions – com protegir-nos al Cloud assegurant el cumpliment normatiu evitant sancions

1. MFA i Centralitzar la visibilitat dels entorns privats, híbrids i multinúvol.
2. Utilitzeu un tallafoc d'aplicacions web per protegir les vostres aplicacions natives del núvol.
3. Implementant un automatisme de cerca d'amenaces que s'actualitzi dinàmicament i de forma continua
4. Utilitzeu capacitats d'intel·ligència d'amenaces per anticipar-se a les properes amenaces i prioritzar de manera eficaç per prevenir-les
5. Mantenir al dia el compliment normatiu aplicable a la industria i territori, i elaborar KPIs de fácil seguiment per la direcció
6. Xifra totes les dades dins del núvol per garantir un flux fluid entre les aplicacions.
7. Aplicar els estàndards de seguretat al núvol amb una solució de gestió de la postura de seguretat al núvol (CSPM).
8. Protegiu la vostra càrrega de treball i contenidors amb una solució de protecció de càrrega de treball al núvol (CWP).
9. Adoptar SASE i Zero-Trust autoritzant l'accés només als usuaris que realment ho necessiten i només als recursos que necessiten. ,
10. Elaborar un pla de resposta a incidents en cas d'incompliment per solucionar la situació, evitar interrupcions operatives i recuperar les dades perdudes.

MOLTES GRÀCIES

ANDORRA DIGITAL

ANC-AD

@anc_ad

@anc-ad

csirt.anc@govern.ad