I´m DevSecOps



The ∞ Saga

CLOUD LEGION

CSA LATAM FORUM 2019

/cloud_legion_ar /company/cloud-legion/



Luciano Moreira

CDSO - Chief DevSecOps strategy Officer

/Luciano_m_cruz /lucianomoreiradacruz/



Christian Ibiri

CEO - Chief Executive Officer

/Christianibiri /christian-ibiri/

Russo Brothers
@Russo_Brothers

Following



1:25 PM - 22 Apr 2019

Russo Brothers
@Russo_Brothers

If you haven't seen Endgame yet, see it this weekend.
The spoiler ban lifts on Monday!
Check out @GMA for the full video...

Traducir Tweet



12:13 p. m. · 2 may. 2019 · Twitter for iPhone

Toda saga tiene un inicio (Cambio)

CSA LATAM FORUM 2019

….El cliente cambió



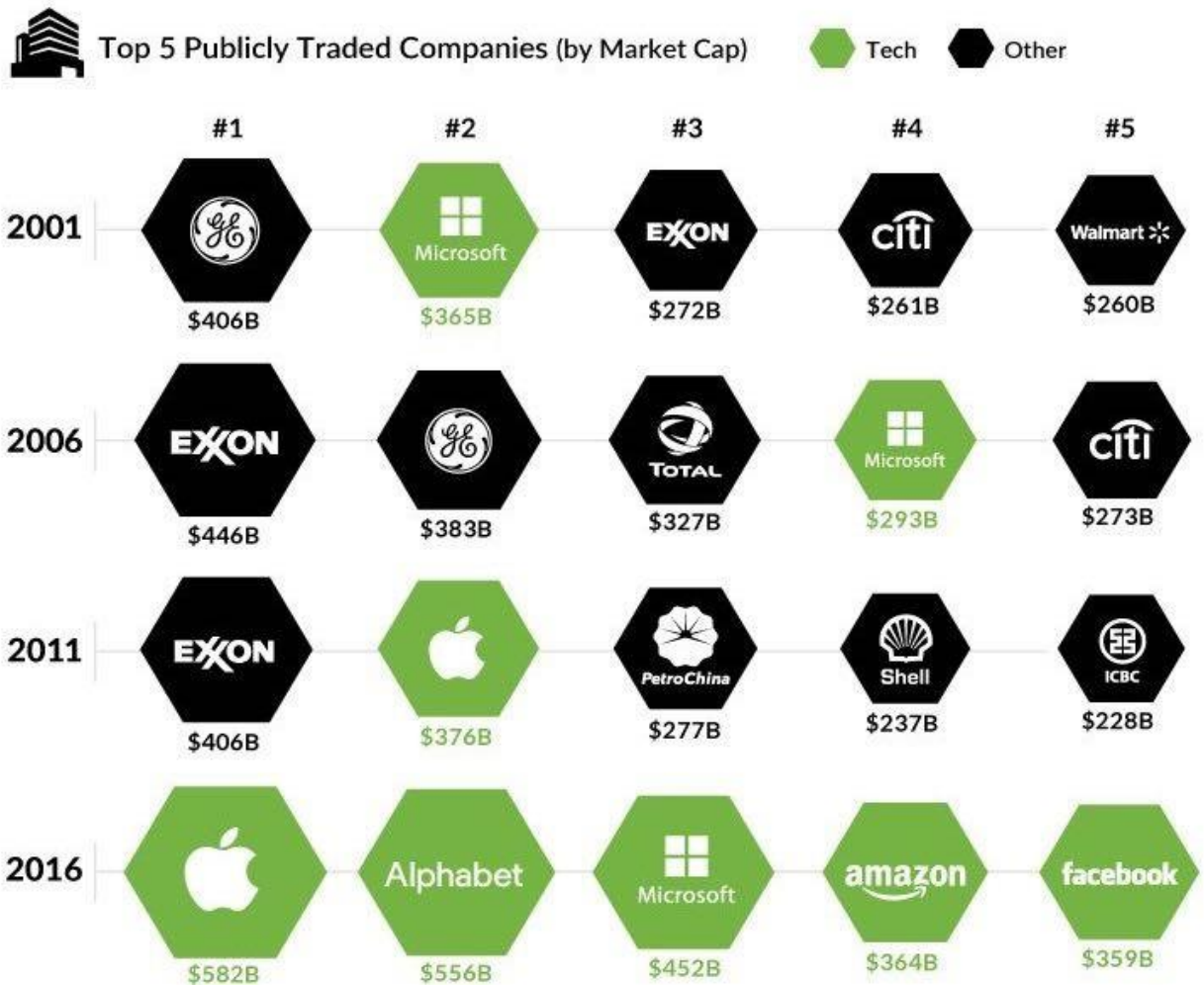
…y es cada vez más exigente!

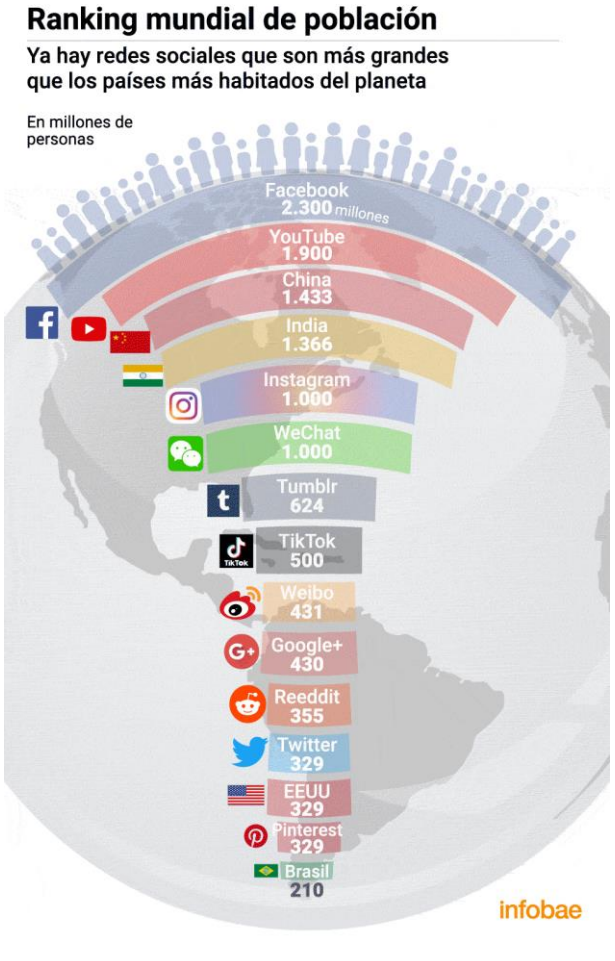
Cambiaron sus expectativas.	No “compra” por nuestro mensaje.	Busca experiencias.	Después comunica y multiplica su experiencia por las redes sociales.


ABURRIDO!!!!
¡TODOS YA SABEMOS ESTO!
¿POR QUÉ DEBERÍA DE IMPORTARME?

Simple…

CSA LATAM FORUM 2019

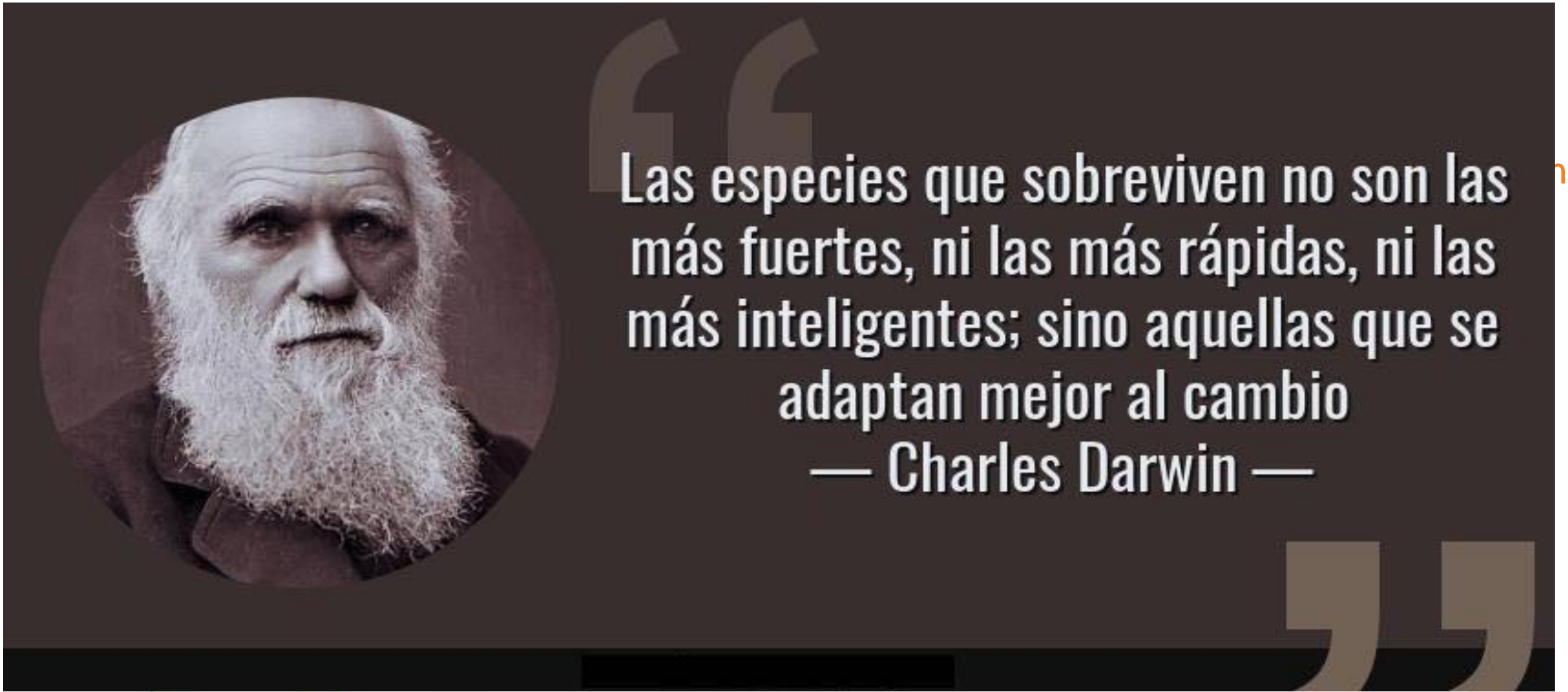




La tecnología y la sociedad evolucionan más rápido que la capacidad de adaptación de las empresas y su operaciones

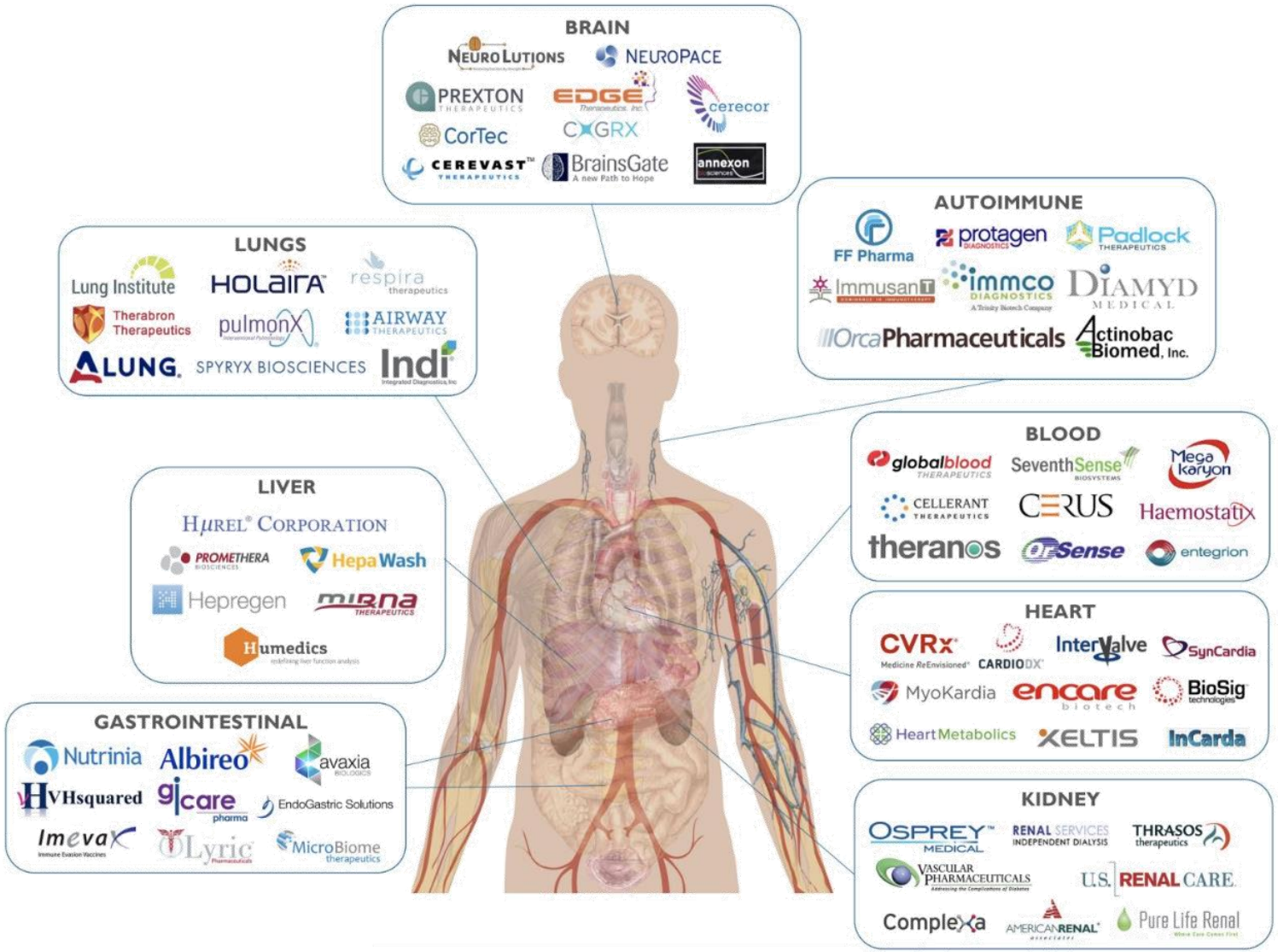
“si, también aplica a los de seguridad”

Simple…


Las especies que sobreviven no son las más fuertes, ni las más rápidas, ni las más inteligentes; sino aquellas que se adaptan mejor al cambio
— Charles Darwin —

Salud

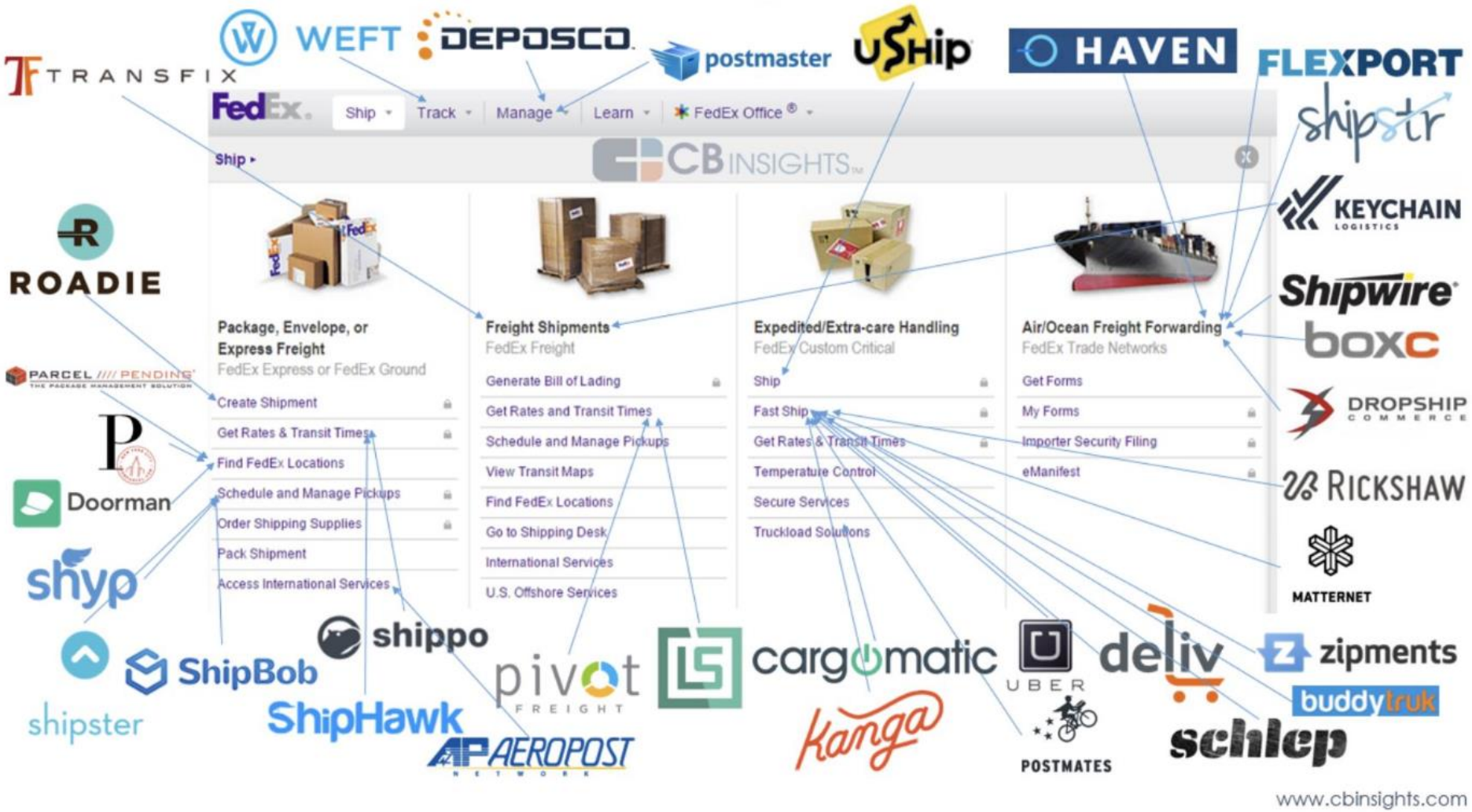
CSA LATAM FORUM 2019



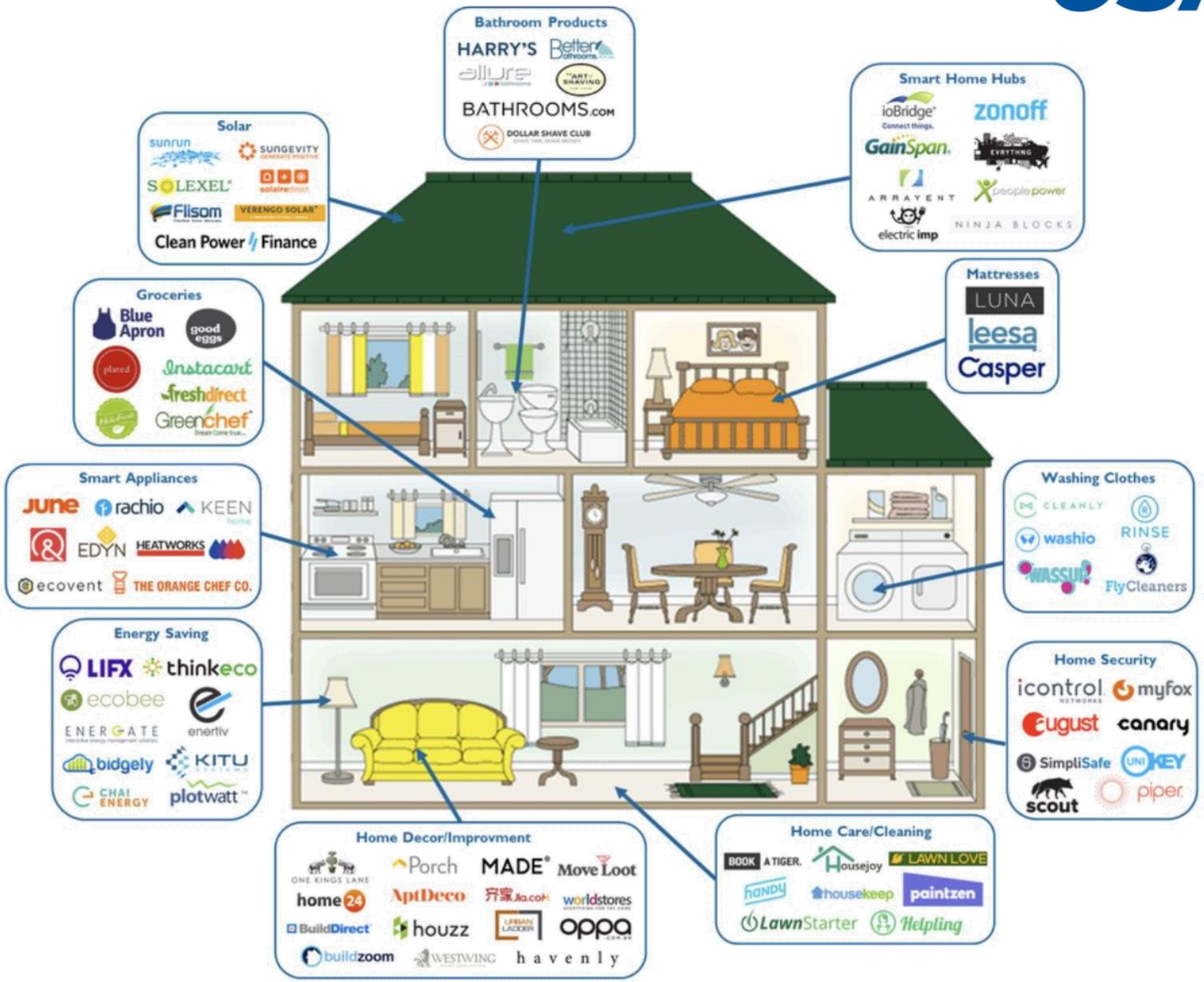
La innovación en la salud no tienen riesgo, yo me cure..



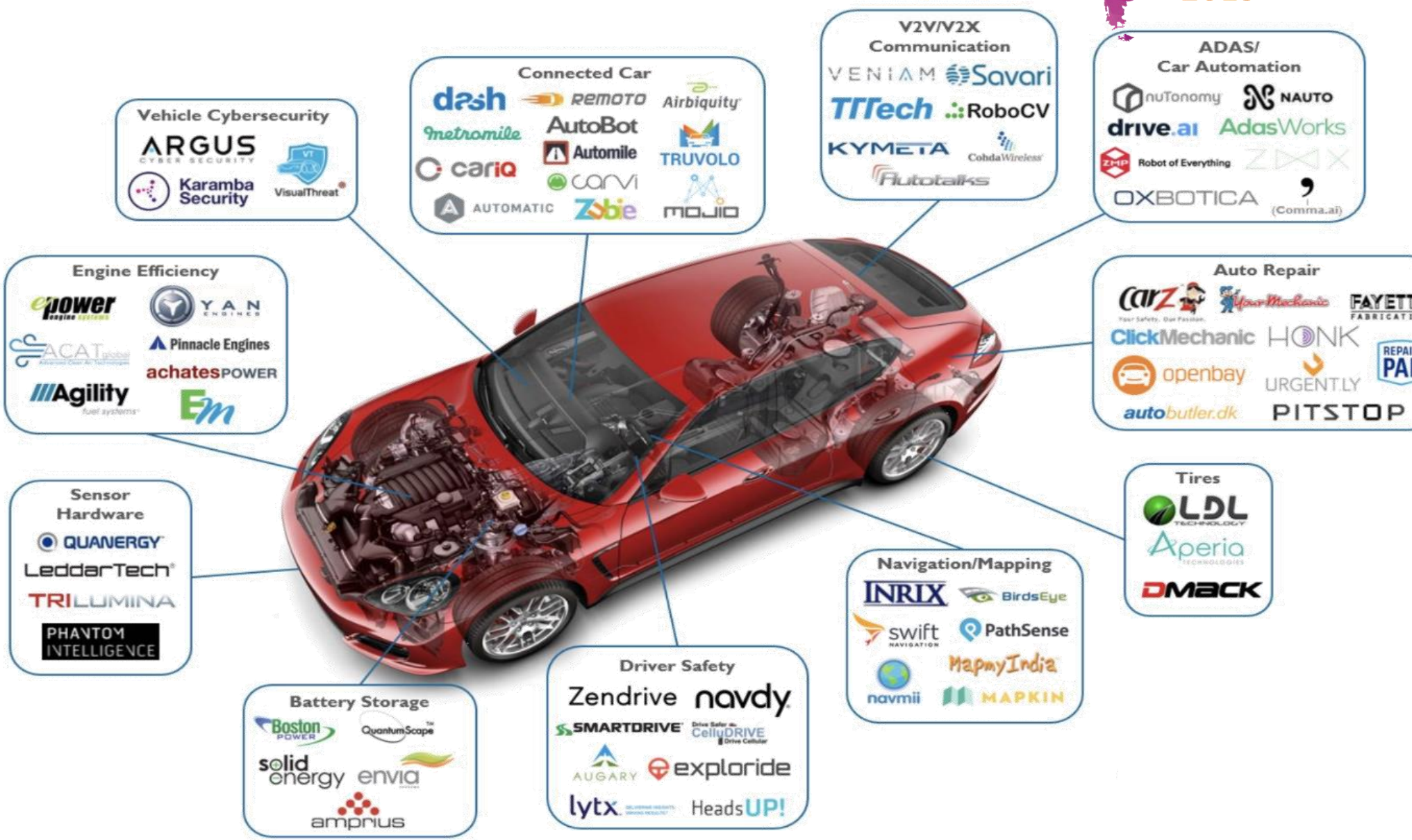
Logística


TRANSFIX
WEFT
DEPOSCO
postmaster
uShip
HAVEN
FLEXPORT
shipstr
FedEx
Ship
Track
Manage
Learn
FedEx Office
CB INSIGHTS
ROADIE
KEYCHAIN LOGISTICS
Shipwire
boxc
PARCEL PENDING
DROPSHIP COMMERCE
Doorman
RICKSHAW
MATTERNET
shyp
shippo
ShipBob
shipster
ShipHawk
pivot FREIGHT
cargomatic
UBER
deliv
zipments
buddytruk
Kanga
schlep
POSTMATES
AEROPOST NETWORK
Package, Envelope, or Express Freight
FedEx Express or FedEx Ground
Create Shipment
Get Rates & Transit Times
Find FedEx Locations
Schedule and Manage Pickups
Order Shipping Supplies
Pack Shipment
Access International Services
Freight Shipments
FedEx Freight
Generate Bill of Lading
Get Rates and Transit Times
Schedule and Manage Pickups
View Transit Maps
Find FedEx Locations
Go to Shipping Desk
International Services
U.S. Offshore Services
Expedited/Extra-care Handling
FedEx Custom Critical
Ship
Fast Ship
Get Rates & Transit Times
Temperature Control
Secure Services
Truckload Solutions
Air/Ocean Freight Forwarding
FedEx Trade Networks
Get Forms
My Forms
Importer Security Filing
eManifest
www.cbinsights.com

Hogar


Bathroom Products
HARRY'S
Better Bathrooms
allure
The Art of Shaving
BATHROOMS.com
DOLLAR SHAVE CLUB
Solar
sunrun
SUNGEVITY
SOLEXEL
solairedirect
Flisom
VERENGO SOLAR
Clean Power Finance
Smart Home Hubs
ioBridge
Connect things.
zonoff
GainSpan
EVRYTHNG
ARRAYENT
peoplepower
electric imp
NINJA BLOCKS
Groceries
Blue Apron
good eggs
plated
Instacart
freshdirect
Hello Fresh
Greenchef
Mattresses
LUNA
leesa
Casper
Smart Appliances
June
rachio
KEEN home
EDYN
HEATWORKS
ecovent
THE ORANGE CHEF CO.
Washing Clothes
CLEANLY
RINSE
washio
WASSUP
FlyCleaners
Energy Saving
LIFX
thinkeco
ecobee
enertiv
ENERGATE
bidgely
KITU
CHAI ENERGY
plotwatt
Home Security
icontrol
NETWORKS
myfox
August
canary
SimpliSafe
UNIKEY
scout
piper
Home Decor/Improvment
ONE KINGS LANE
Porch
MADE
Move Loot
home 24
AptDeco
worldstores
BuildDirect
houzz
URBAN LADDER
oppa
buildzoom
WESTWING
havenly
Home Care/Cleaning
BOOK A TIGER.
Housejoy
LAWN LOVE
handy
housekeep
paintzen
LawnStarter
Helpling

Auto


Vehicle Cybersecurity
ARGUS
Karamba Security
VisualThreat
Connected Car
dash
REMOTO
Airbiquity
Metromile
AutoBot
Automile
TRUVOLO
cariq
carvi
AUTOMATIC
Zubie
mojio
V2V/V2X Communication
VENIAM
Savari
TTTech
RoboCV
KYMETA
CohdaWireless
Autotalks
ADAS/ Car Automation
nuTonomy
NAUTO
drive.ai
AdasWorks
Robot of Everything
OXBOTICA
(Comma.ai)
Engine Efficiency
epower
YAN
ACAT
Pinnacle Engines
achatesPOWER
Agility
Em
Auto Repair
carZ
YourMechanic
ClickMechanic
HONK
openbay
URGENTLY
autobutler.dk
PITSTOP
Sensor Hardware
QUANERGY
LeddarTech
TRILUMINA
PHANTOM INTELLIGENCE
Tires
LDL TECHNOLOGY
Aperia
DMACK
Navigation/Mapping
INRIX
BirdsEye
swift
PathSense
MapmyIndia
navmii
MAPKIN
Battery Storage
Boston POWER
QuantumScape
solid energy
envia
amprius
Driver Safety
Zendrive
navdy
SMARTDRIVE
CellyDRIVE
AUGARY
exploride
lytx
HeadsUP!

Banca


Pave
SparkFund
Polly Portfolio
STREET SHARES
KAPITALL
ARTIVEST
WiseBanyan
PERSONAL CAPITAL
Propellr
everplans
LOAN HERO
motif INVESTING
Stockpile
wealthfront
SprinkleBit
SIGFIG
smartasset
aboutLife
WELLS FARGO
Personal
robinhood
Aspiration
Betterment
Financial Education
nerdwallet
LEARNVEST
Patch of Land
ADF
EVEN FINANCIAL
Banking
Loans and Credit
Insurance
Investing and Retirement
Wealth Management
Rewards and Benefits
AssetAvenue
loanlogics
Stilt
zest finance
View Your Accounts
Account Summary
Username
Password
Go
Save Username
Forgot Password/Username?
Buying a house?
Estimate how much you may be able to borrow
Get Prequalified
sindeo
FUNDTHATFLIP
LoanNow
Landed
LendingHome
INSIKT
lenda
Figtree
blooom
SELFLENDER
CoverHound
Ledge.
thezebra
AVANT CREDIT
Upstart
earnest
TUITION.IO
LendUp
Elevate
College AVE
SoFi
Going to College
Home Lending
Banking Made Easy
Credit Karma
OPPORTUN
PROSPER
Cumulus
Moven
Zebit
SnapCheck
Payoff
digit
Bank wherever life takes you
Whether you're choosing a checking account, banking on the go, or managing your spending, Wells Fargo makes it easy for you to manage your everyday banking.
credit sesame
Everyday Checking
Open a new checking account online in minutes
Get Started
bread
PayNearMe
chime
Go To Banking Made Easy
covestor
Remitly
regalii
affirm
thumzap
RUSHCARD
lendio
beyonic
Juvo
FUNDBOX
LendingRobot
Make saving money simpler
Automatically save with a Way2Save® Savings account
Learn More
uphold
rize
EMBROKER
varo
SNAPADVANCES
MoCaFi
PayActiv
BOOST UP
Penny
SimplyInsured
able
BOND STREET
WB21
coverwallet
forusall
GUSTO
BEHALF
ApplePie CAPITAL
P2Binvestor
BROKE
acorns
insureon
fundera
Even
BILL GUARD
Lumity
JUSTWORKS.
Manage Payroll and Employees
Financing and Credit
Make & Receive Payments
Get Started with Checking
GoCo
Namely
wave
zuora
Captain401
next insurance
CAN CAPITAL
Kabbage
C2FO
flint
TRANSACTIS
ZENEFITS
Dealstruck
eShares
Credit Junction
BlueVine
InvestNextDoor
CREDIBLY
Bill.com
Mozido
ROMIT
mobeam

Alimentos


ENERGY DRINKS
KILL CLIFF
SAMBAZON
FRS ENERGY + ENDURANCE
MATI
fuelfor FIRE
GLUKOS
DAIRY
good culture
COTTAGE CHEESE, BUT BETTER
elli
CHEVOO
the chaat co
maia
SODA
spindrift
Q TONIC
Sipp
Zevia
CHIPS
PRIMIZIE
THICK CUT CRISPBREADS
CHIRPS
EAT WHAT BUGS YOU
POP!
MEAT & DAIRY SUBSTITUTES
ripple
WayFare
Hampton Creek
BEYOND MEAT
IMPOSSIBLE
Perfect Day
MIYOKO'S KITCHEN
kite hill
MEMPHIS MEATS
GOOD KARMA
Clara Foods
daiya
deliciously dairy free
Heidi Ho
FROZEN DESSERTS
yasso
Jala!
HALO TOP
oppo
INDULGE HEALTHY
Ruby Rockets
JC's
BABY FOOD
once upon a farm
nurturme
CONDIMENTS
SIR KENSINGTON'S
TESSEMAE'S
& hummus
MEDITERRANEAN FOODS
BANDA
CANDY
ALTER ECO
UNREAL
TCHO
sweetriot
OCHO Candy
theo
Raaka
SIMPLY GUM
Nib Mor
boomf
TEA
Numi ORGANIC TEA
ROOIBEE RED TEA
Bhakti
GUAYAKI YERBA MATE
TEABOX
ZEST TEA
tiesta tea
RUNA
LIQUID MEALS
soylent
ambronite
mixo
rumble
Feed.
BAKING & SPICES
Nutek Food Science
KIKI'S
MANINI'S
DELICIOUS, FRESH, & GLUTEN FREE
Numi
Hail Merry
PROTEIN BARS
HEALTH WARRIOR
exo
CRICKET FLOUR
ALOHA
REGRAINED
EAT BEER.
KOMBUCHA
HEALTH-ADE KOMBUCHA
GoodBelly
LIVE BEVERAGES
humm kombucha
revive kombucha
MEAT & FISH
PRE
CHEF'S CUT REAL JERKY
Hip Chick Farms
WALDEN LOCAL MEAT CO.
PERKY JERKY
NEW WAVE FOODS
SOUPS
KITCHEN22
tio gazpacho
COFFEE
CHAMELEON COLD-BREW
CALIFIA FARMS
BLUE BOTTLE
HIGH Brew COFFEE
FRUIT & HERBAL DRINKS
WTR MLN WTR
coco libre
hint
drink water, not sugar
TEMPLE TURMERIC
suja
maple
KULI KULI
cheribundi
VITA COCO
FRUIT & VEGETABLE SNACKS
banana
peeled SNACKS
SKINNY DIPPED almonds
RHYTHM SUPERFOODS
hourish SNACKS
SOUL SPROUT
nomva
better bean
HALO
SAHALE SNACKS
Farmwise
dang
HALFPOPS
BRAMI
PACKAGED MEALS
LOVE THE WILD
bueN sabor
SAFFRON ROAD
Hilary's
LÜVO
fishpeople
hungryroot

Campo


FARM MANAGEMENT SOFTWARE
Farmdok
landmapp
AEGRO
scoutpro
Granular
Agworld
agrivi
conservis
Cropin
trecker.com
PICKTRACE
FarmLogs
AgriWebb
ONFARM
NEXT GEN FARMS
BOWERY
alesca life
FREIGHT FARMS
FRESH BOX FARMS
BRIGHT FARMS
GREEN SENSE FARMS
AeroFarms
GOTHAM GREENS
PRECISION AGRICULTURE AND PREDICTIVE ANALYTICS
agronóstico
AGRIBLE
GAMAYA
Strider
GeoVisual
agrilyst
S4
Observe
CropMetrics
adapt-N
FARMERS
Premier Crop Systems
bovcontrol
CropZilla
MyAgData.com
AGRALOGICS
prospera
aWhere
ec2ce
FluroSat
ANIMAL DATA
AAD
Farmnote
stellapps
Mastiline
TL Biolabs
Connecterra
COWLAR
Moocall
MARKETPLACES
AgroStar
Agriconomie
LA RUCHE QUI DIT OUI !
Aggrigator
EM3
YAGRO
ROBOTICS AND DRONES
mavrx
FarmBot
AIRWOOD
RAPTOR MAPS
HARVEST CROO ROBOTICS
BLUE RIVER TECHNOLOGY
SkySquirrel
SKYCISION
LEADING EDGE
TerrAvion
RESSON
abundant ROBOTICS
ceresimaging
SENSORS
Centaur
SLANTRANGE
grownetics
motorleaf
pycno
SPENSA
amber AGRICULTURE
Saturas
Acuity Agriculture
FieldIn
FARMOBILE
Grassometer
Phytech
FarmersEdge
ARABLE
SMART YIELDS
flux
GardenSpace
semios
Sencrop
SMART IRRIGATION
flowius
Tevatronic
livn
HORTAU
SIMPLIFIED IRRIGATION
Sprinkl
HydroPoint
SMART FARM.
PowWow
cropx
AquaSpy
EDYN
PLANT DATA/ANALYSIS
CiBO
TRACE GENOMICS
BENSON HILL

DISRUPCIÓN DIGITAL

CSA LATAM FORUM 2019

Nuestra vida definida por la tecnología

“Software”

“Empiezas con algo puro, algo emocionante, y luego llegan los errores, los compromisos” - Tony Stark en Iron Man 3.

¿Como termina esta oración?



?


Your shield has been hacked.

Your shield has been hacked.

Security

After years of warnings, mobile network hackers exploit SS7 flaws to drain bank accounts

O2 confirms online thefts using stolen 2FA SMS codes

By Iain Thomson in San Francisco 3 May 2017 at 20:02 48 SHARE



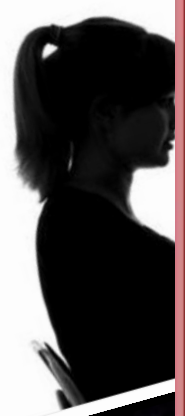
Your shield has been hacked.

Security

After years of warnings, mobile network hackers exploit SS7 flaws to drain bank accounts

O2 confirms online thefts using stolen 2FA SMS codes

By Iain Thomson in San Francisco 3 May



Wana Decrypt0r 2.0

Ooops, your files have been encrypted!

English

What Happened to My Computer?

Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am

Payment will be raised on
5/16/2017 00:47:55
Time Left
02:23:57:37

Your files will be lost on
5/20/2017 00:47:55
Time Left
06:23:57:37

About bitcoin
How to buy bitcoins?
Contact Us

bitcoin ACCEPTED HERE

Send $300 worth of bitcoin to this address:

12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

Copy

Check Payment

Decrypt

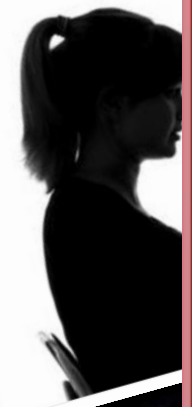
Your shield has been hacked.

Security

After years of warnings, mobile network hackers exploit SS7 flaws to drain bank accounts

O2 confirms online thefts using stolen 2FA SMS codes

By Iain Thomson in San Francisco 3 May



Wana Decrypt0r 2.0

Ooops, your files have been encrypted!

What Happened to My Computer?

Your important files are encrypted.

Many of your documents, photos, videos, databases and other files are no accessible because they have been encrypted. Maybe you are busy looking recover your files, but do not waste your time. Nobody can recover your f our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But y not so enough time.

You can decrypt some of your files for free. Try now by clicking <Decrypt>.

But if you want to decrypt all your files, you need to pay.

You only have 3 days to submit the payment. After that the price will be doubled

Also, if you don't pay in 7 days, you won't be able to recover your files forever.

We will have free events for users who are so poor that they couldn't pay in 6 mo

How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.

Please check the current price of Bitcoin and buy some bitcoins. For more informatio click <How to buy bitcoins>.

And send the correct amount to the address specified in this window.

After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am

Payment will be raised on

5/16/2017 00:47:55

Time Left

02:23:57:37

Your files will be lost on

5/20/2017 00:47:55

Time Left

06:23:57:37

About bitcoin

How to buy bitcoins?

Contact Us

bitcoin ACCEPTED HERE

Send $300 worth of bitcoin to this address:

12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

Copy

Check Payment

Decrypt

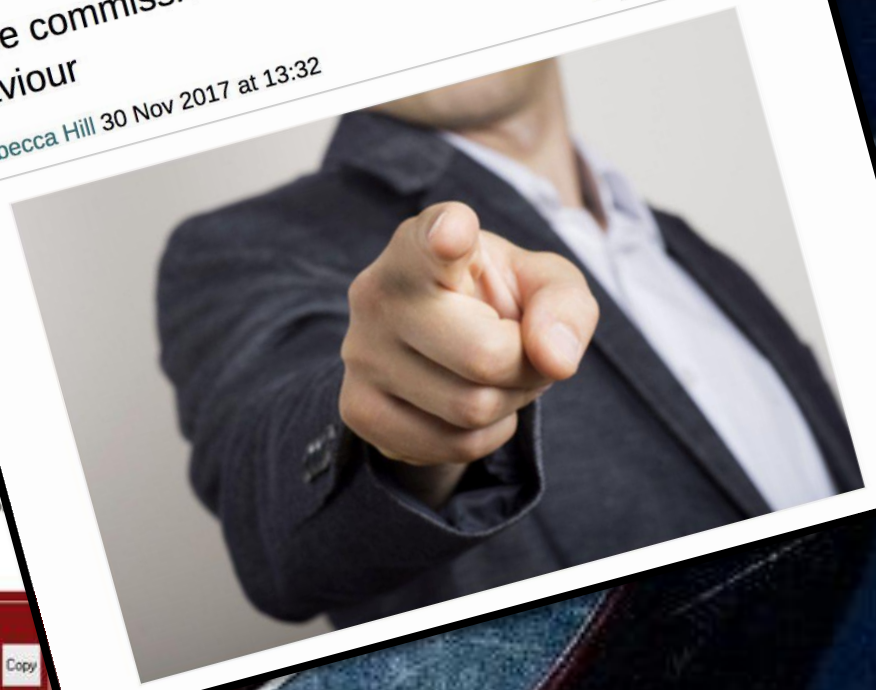
Uber hack: EU data protection bods launch taskforce

Justice commissioner slams biz for 'irresponsible' behaviour

By Rebecca Hill 30 Nov 2017 at 13:32

6

SHARE



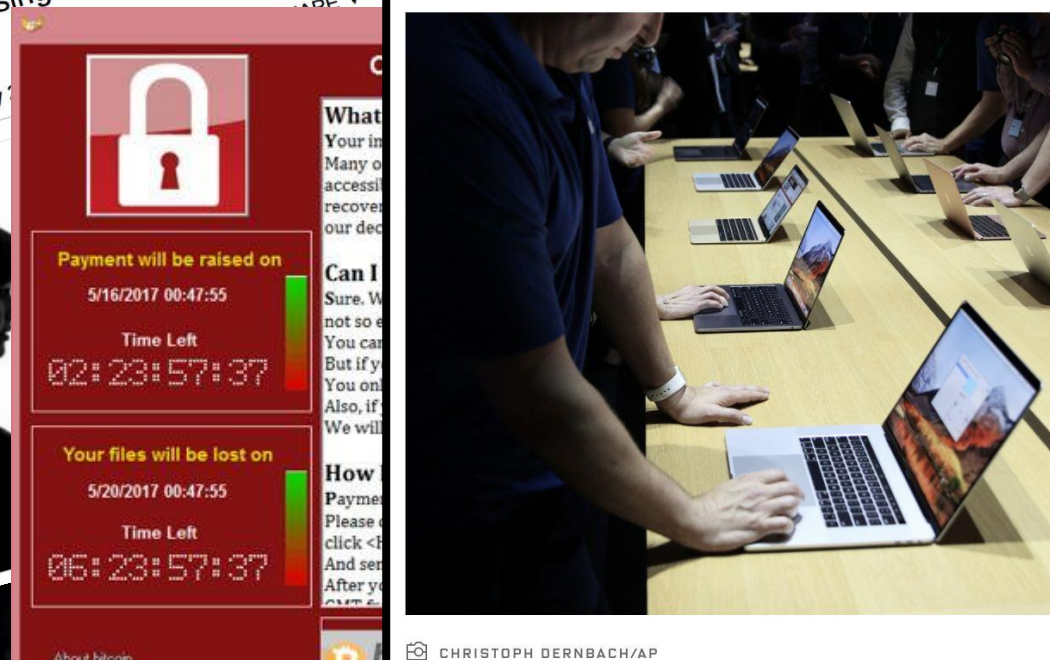
Your shield has been hacked.

Security

After years of warnings, mobile network hackers exploit SS7 flaws to drain bank accounts

O2 confirms online thefts using stolen 2FA SMS codes

By Iain Thomson in San Francisco 3 May



ANDY GREENBERG SECURITY 11.28.17 05:47 PM

ANYONE CAN HACK MACOS HIGH SIERRA JUST BY TYPING "ROOT"

CHRISTOPH DERNBACH/AP

a protection bods

slams biz for 'irresponsible'

6 SHARE

13:32



Your shield has been hacked.

Security

After years
network h
drain ba

O2 confirm
codes

By Iain Thom

ACTUALIDAD · HACKING · PRIVACIDAD

Consiguen robar las tarjetas de crédito de 380.000 clientes de British Airways

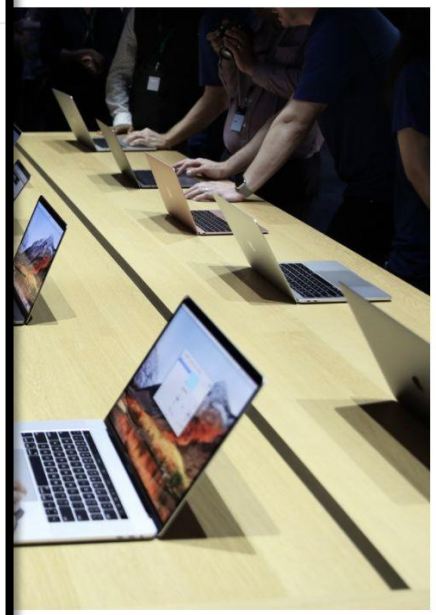
7 de septiembre, 2018



La conocida aerolínea británica **British Airways** ha reconocido y confirmado un **robo de datos** que ha expuesto los datos

ANDY GREENBERG SECURITY 11.28.17 05:47 PM

ANYONE CAN HACK MACOS HIGH
TYPING



How to buy bitcoins?

Contact Us

Check Payment

Decrypt

a protection bods

slams biz for 'irresponsible'

6 SHARE

13:32



Your shield has been hacked.

Security

After years
network h
drain ba

O2 confirm
codes

By Iain Thom

ANDY GREENBERG SECURITY 11.28.17 05:47 PM

ANYONE CAN HACK MACOS HIGH
TYPING

ACTUALIDAD · HACKING · PRIVACIDAD

Consiguen robar las tarjetas de crédito de 380.000 clientes de British Airways

7 de septiembre, 2018



La conocida aerolínea británica **British Airways** ha reconocido y confirmado un **robo de datos** que ha expuesto los datos

How to buy bitcoins?

Contact Us

Check Payment

Decrypt

tion bods

SEGURIDAD

El hackeo a Facebook comprometió la información de 30 millones de cuentas

14 de octubre, 2018



El hackeo a Facebook del mes pasado, el **error de seguridad más grave de la historia de la compañía**, comprometió la información personal de 30 millones de usuarios, según la nueva información facilitada por el vicepresidente de Facebook, Guy

Your shield has been hacked.

Fuga masiva de datos en Gearbest: cambia ya tu contraseña

15 de marzo, 2019

Gearbest
QUALITY · AFFORDABLE · FUN

Una nueva brecha de seguridad ha desatado el **«pánico en los mercados»**. La compañía afectada en este caso ha sido Gearbest, una de las plataformas chinas de comercio electrónico más populares en países como España.

Como indican en TechCrunch, un servidor mal configurado en la CPD de la empresa asiática ha provocado que millones de datos de usuarios y clientes se hayan estado filtrando en Internet desde hace semanas. Tan mal configurado estaba, que ni siquiera estaba protegido con contraseña.

ANDY GREENBERG SECURITY 11.28.17 05:47 PM

ANYONE CAN HACK MACOS HIGH
TYPING

de crédito de 380.000 clientes de



conocido y confirmado un **robo de datos** que ha expuesto los datos

SEGURIDAD

El hackeo a Facebook comprometió la información de 30 millones de cuentas

14 de octubre, 2018



El hackeo a Facebook del mes pasado, el **error de seguridad más grave de la historia de la compañía**, comprometió la información personal de 30 millones de usuarios, según la nueva información facilitada por el vicepresidente de Facebook, Guy

Contact Us

Check Payment

Decrypt

Your shield has been hacked.

Fuga masiva de datos en Gearbest: cambia ya tu contraseña

15 de marzo, 2019

Gearbest
QUALITY · AFFORDABLE · FUN

Una nueva brecha de seguridad ha desatado el **«pánico en los mercados»**. La compañía afectada en este caso ha sido Gearbest, una de las plataformas chinas de comercio electrónico más populares en países como España.

Como indican en TechCrunch, un servidor mal configurado en la CPD de la empresa asiática ha provocado que millones de datos de usuarios y clientes se hayan estado filtrando en Internet desde hace semanas. Tan mal configurado estaba, que ni siquiera estaba protegido con contraseña.

Las fugas de datos de usuario son una epidemia: 590 millones en China y 540 millones de Facebook

5 de abril, 2019



Parece que tendremos que acostumbrarnos a fugas de datos de usuario masivas a la vista de que se repiten semana a semana, a pesar que **incumplen todos los compromisos éticos y legales de protección de datos** y derecho a la privacidad de los usuarios. Estos últimos días se han conocido otras dos de las gordas.

Curriculums en China

Compañías chinas han filtrado la friolera de **590 millones de curriculums vitae** en los primeros tres meses del año, según leemos en ZDNet. La mayoría de las fugas se han producido debido a que las bases de datos MongoDB y los servidores ElasticSearch están mal asegurados y se han dejado expuestos en línea sin una contraseña, o han terminado en línea luego de errores inesperados del cortafuegos.

Parece que la fuga está limitada a China, pero el medio apunta que se trata de una señal preocupante de que las compañías de Recursos Humanos del gigante asiático no están tomando en serio la seguridad de sus servidores.

PM

CK MACOS HIGH
TYPING

tion bods

SEGURIDAD

El hackeo a Facebook comprometió la información de 30 millones de cuentas

14 de octubre, 2018



El hackeo a Facebook del mes pasado, el **error de seguridad más grave de la historia de la compañía**, comprometió la información personal de 30 millones de usuarios, según la nueva información facilitada por el vicepresidente de Facebook, Guy

Contact Us

Check Payment

Decrypt

Your shield has been hacked.

Fuga masiva de datos en Gearbest: cambia ya tu contraseña

15 de marzo, 2019

Gearbest
QUALITY · AFFORDABLE · FUN

Una nueva brecha de seguridad ha desatado el **«pánico en los mercados»**. La compañía afectada en este caso ha sido Gearbest, una de las plataformas chinas de comercio electrónico más populares en países como España.

Como indican en TechCrunch, un servidor mal configurado en la CPD de la empresa asiática ha provocado que millones de datos de usuarios y clientes se hayan estado filtrando en Internet desde hace semanas. Tan mal configurado estaba, que ni siquiera estaba protegido con contraseña.

Las fugas de datos de usuario son una epidemia: 590 millones en China y 540 millones de Facebook

5 de abril, 2019



Parece que tendremos que acostumbrarnos a fugas de datos de usuario masivas a la vista de que se repiten semana a semana, a pesar que **incumplen todos los compromisos éticos y legales de protección de datos** y derecho a la privacidad de los usuarios. Estos últimos días se han conocido otras dos de las gordas.

Curriculums en China

Compañías chinas han filtrado la friolera de **590 millones de curriculums vitae** en los primeros tres meses del año, según leemos en ZDNet. La mayoría de las fugas se han producido debido a que las bases de datos MongoDB y los servidores ElasticSearch están mal asegurados y se han dejado expuestos en línea sin una contraseña, o han terminado en línea luego de errores inesperados del cortafuegos.

Parece que la fuga está limitada a China, pero el medio apunta que se trata de una señal preocupante de que las compañías de Recursos Humanos del gigante asiático no están tomando en serio la seguridad de sus servidores.

Segunda mayor fuga de datos de la historia: 773 millones de cuentas de correo

18 de enero, 2019



El investigador de seguridad y fundador del sitio web de infracciones Have I Been Pwned, ha revelado una base de datos que incluye **773 millones de cuentas de correo electrónico y 21 millones de contraseñas únicas robadas,** que a buen seguro se han estado utilizando en ataques informáticos automatizados de relleno de credenciales.

Es la segunda mayor fuga de datos de la historia después de la de Yahoo! con casi 3.000 millones de cuentas afectadas, aunque hay que concretar que se trata de una **compilación de otras bases de datos más pequeñas ya filtradas**, según explica Troy Hunt.

Denominada como 'Colection #1' por su descubridor, la compilación estaba formada por un conjunto de **12.000 archivos con un tamaño total de 87 Gbytes y casi 2.700 mil millones de registros**, sumando 1.160 millones de combinaciones únicas entre las direcciones de correo y las contraseñas, lo que significa que la lista cubre a las mismas personas varias veces, pero en muchos casos con contraseñas diferentes.



...idad más grave de la historia de la compañía, comprometió la ...nueva información facilitada por el vicepresidente de Facebook, Guy

Contact Us

Check Payment

Decrypt

Your shield has been hacked.

Fuga masiva de datos en
tu contraseña
15 de marzo, 2019

Una nueva brecha de seguridad ha
mercados». La compañía afectada
Gearbest, una de las plataformas cl
electrónico más populares en paise

Como indican en TechCrunch, un s
CPD de la empresa asiática ha pro
de usuarios y clientes se hayan est
desde hace semanas. Tan mal conf
siquiera estaba protegido con contr

TECNOLOGÍA CIENCIA MÓVILES EMPRENDEDORES APPS INTERNET BLOGS

UN ATAQUE SIMILAR A WANNACRY

Everis y Prisa Radio sufren un grave ciberataque que secuestra sus sistemas

Prisa Radio y varias consultoras tecnológicas como Everis están sufriendo serios ciberataques. Es un 'ransomware' que secuestra archivos y pide un rescate en bitcoins



(EFE)

M. A. MÉNDEZ - GUILLERMO CID -
TAGS RANSOMWARE CIBERATAQUE – CADENA SER
TIEMPO DE LECTURA 5 min

04/11/2019 11:56 - ACTUALIZADO: 04/11/2019 20:44

Ad closed by Google
Stop seeing this ad
Why this ad? ⓘ

Contact Us | Check Payment | Decrypt

Segunda mayor fuga de datos de la historia:
773 millones de cuentas de correo
18 de enero, 2019



El investigador de seguridad y fundador del sitio web de infracciones Have I Been Pwned, ha revelado una base de datos que incluye **773 millones de cuentas de correo electrónico y 21 millones de contraseñas únicas robadas,** que a buen seguro se han estado utilizando en ataques informáticos automatizados de relleno de credenciales.

Es la segunda mayor fuga de datos de la historia después de la de Yahoo! con casi 3.000 millones de cuentas afectadas, aunque hay que concretar que se trata de una **compilación de otras bases de datos más pequeñas ya filtradas**, según explica Troy Hunt.

Denominada como 'Colection #1' por su descubridor, la compilación estaba formada por un conjunto de **12.000 archivos con un tamaño total de 87 Gbytes y casi 2.700 mil millones de registros**, sumando 1.160 millones de combinaciones únicas entre las direcciones de correo y las contraseñas, lo que significa que la lista cubre a las mismas personas varias veces, pero en muchos casos con contraseñas diferentes.

tió la información de 30 millones



idad más grave de la historia de la compañía, comprometió la
nueva información facilitada por el vicepresidente de Facebook, Guy

Your shield has been hacked.

Friday, 06 Sep, 7.11 pm
Republic TV

REPUBLIC. R.

ENTERTAINMENT

Iron Man Robert Downey Jr's Instagram Hacked, Fans Suspect UltronFans suspect Ultron'No giveaway?': Fans disappointedRobert Downey Jr set to return as Iron Man for 'Marvel' spinoff



Hack:

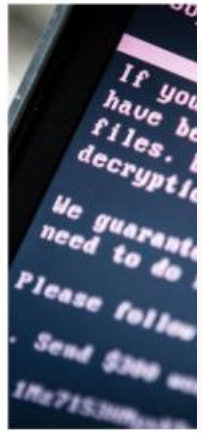
Iron Man Robert Downey Jr's Instagram handle is hacked, the actor announced.

Woah! Looks like someone just overpowered Stark Technologies and hacked Iron Man Robert

TECNOLOGÍA CIENCIA MÓVILE

Everis y l
ciberataqu

Prisa Radio y varias consul
'ransomv



(EFE)

Anterior

M. A. MÉNDEZ - GUILLERMO CID

TAGS RANSOMWARE CIBERATAQUE – CADENA DE

TIEMPO DE LECTURA

04/11/2019 11:56 -

Contact Us

Check Payment

Decrypt

Fuga masiva de datos en
tu contraseña
15 de marzo, 2019

Una nueva brecha de seguridad ha
mercados». La compañía afectada
Gearbest, una de las plataformas cl
electrónico más populares en paise

Como indican en TechCrunch, un s
CPD de la empresa asiática ha prov
de usuarios y clientes se hayan esta
desde hace semanas. Tan mal conf
siquiera estaba protegido con contr

ria:

le

ciales.

s de la

ión de
in

00 mil

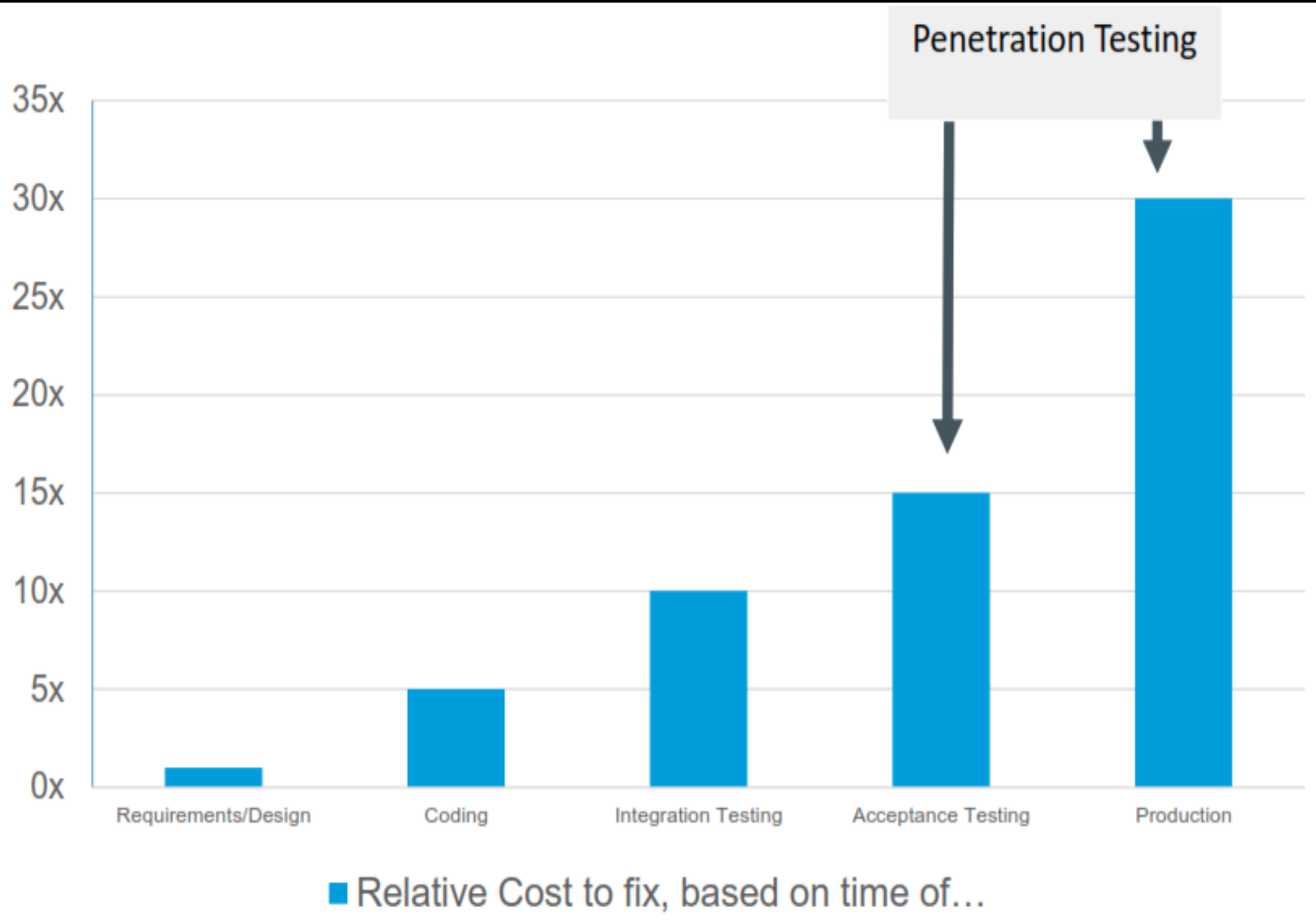
as
nas
aseñas

bods

tió la información de 30 millones



idad más grave de la historia de la compañía, comprometió la
nueva información facilitada por el vicepresidente de Facebook, Guy


Penetration Testing
35x
30x
25x
20x
15x
10x
5x
0x
Requirements/Design
Coding
Integration Testing
Acceptance Testing
Production
Relative Cost to fix, based on time of…

COST OF A DATA BREACH

Sensitive Data Continues to Exit Companies and Cost Millions

Global data breach costs climbed slightly last year

$136

average cost per data breach

$130

U.S. businesses paid an average cost of $5.4 million per data breach

that's $188 per record*



No olvidemos de los errores internos….

CSA LATAM FORUM 2019

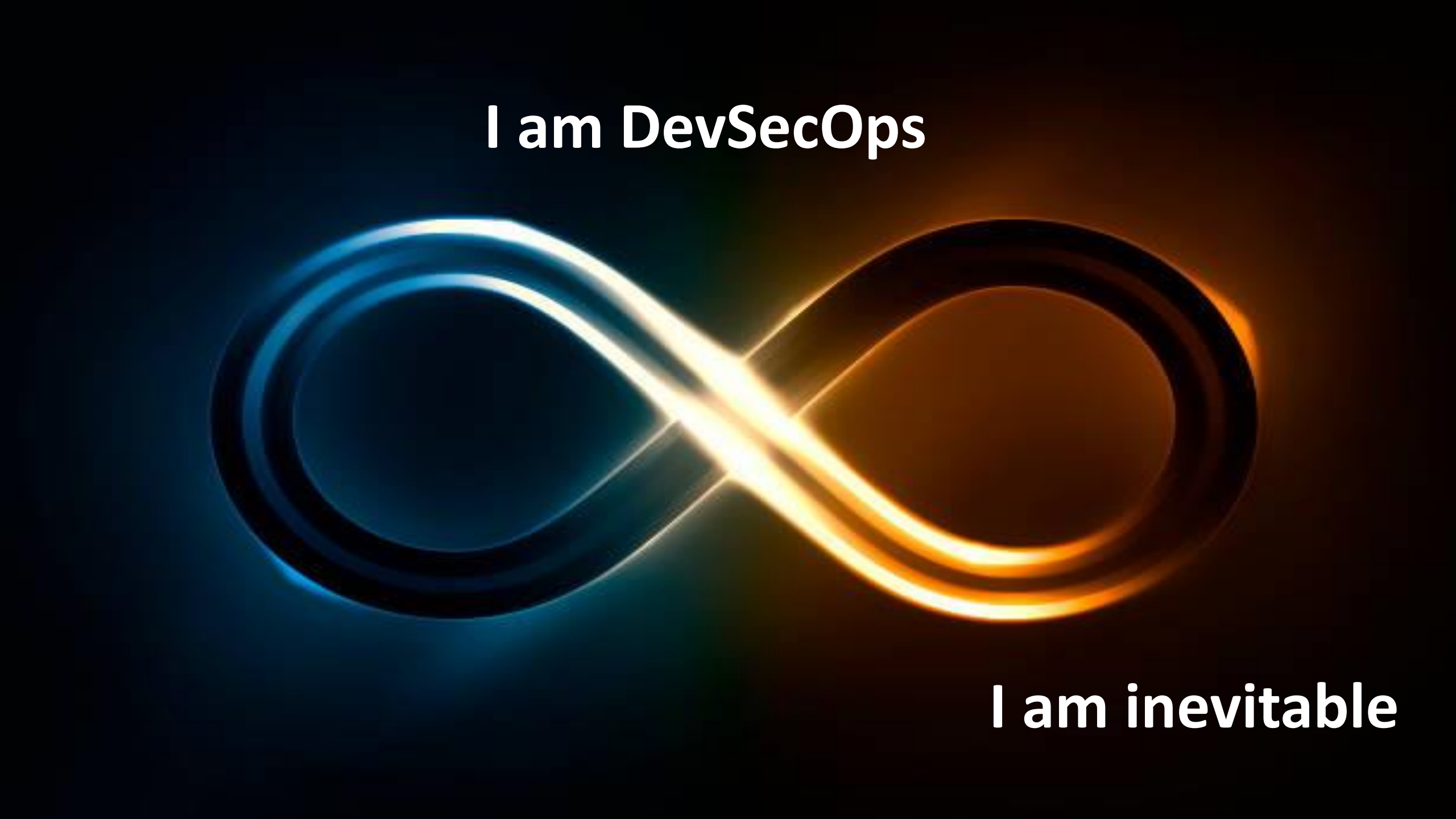


No olvidemos de los errores internos….

CSA LATAM FORUM 2019



I am DevSecOps



I am inevitable

DevSecOps Tools landscape

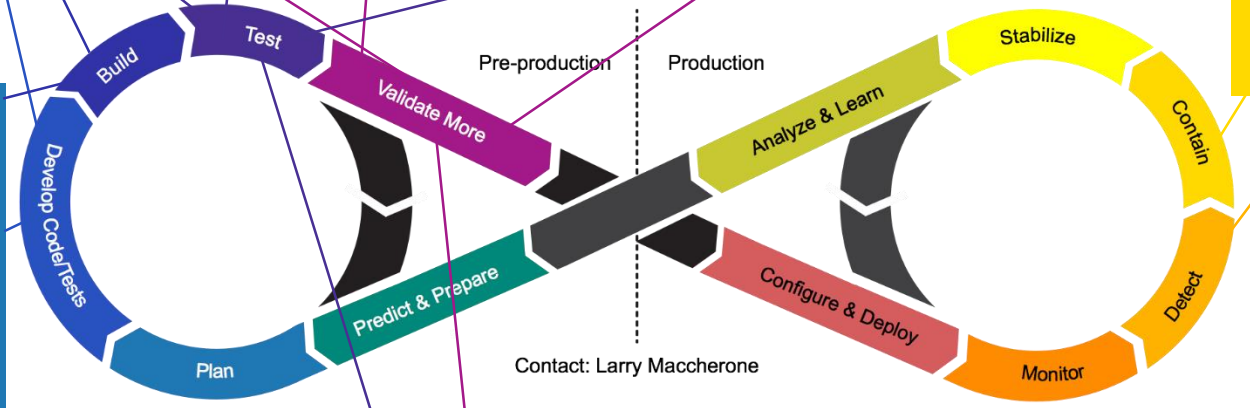
Static Analysis (aka SAST)
- Looks at source code
- Data/control flow analysis
- Prone to false positives
- Rapid feedback for developers
- Code fix suggestions

Dynamic
- Instruments app (to varying degrees)
- Exercises app via UI/API
- Zero? false positives
- Hard to instrument?
- High false negatives
- Report is an exploit
- Sometimes hard to find code to remediate

Fuzzing
- Instruments app (to varying degrees)
- Sends unexpected input at API
- Looks at response and instrumentation output
- Great for testing protocols like SIP
- Good for REST APIs
- Potentially long run times
- Hard to find code to remediate

Runtime Application Security Protection (RASP)
- Reports on "bad" behavior
- Can abort transaction or kill process to protect

Software Composition Analysis (SCA)
- Identifies dependency and version
- Checks CVE/NVD + … for reported vulnerabilities
- Proposes version/patch to remediate
- Checks license vs policy
- Runs fast
- Some have firewall mode

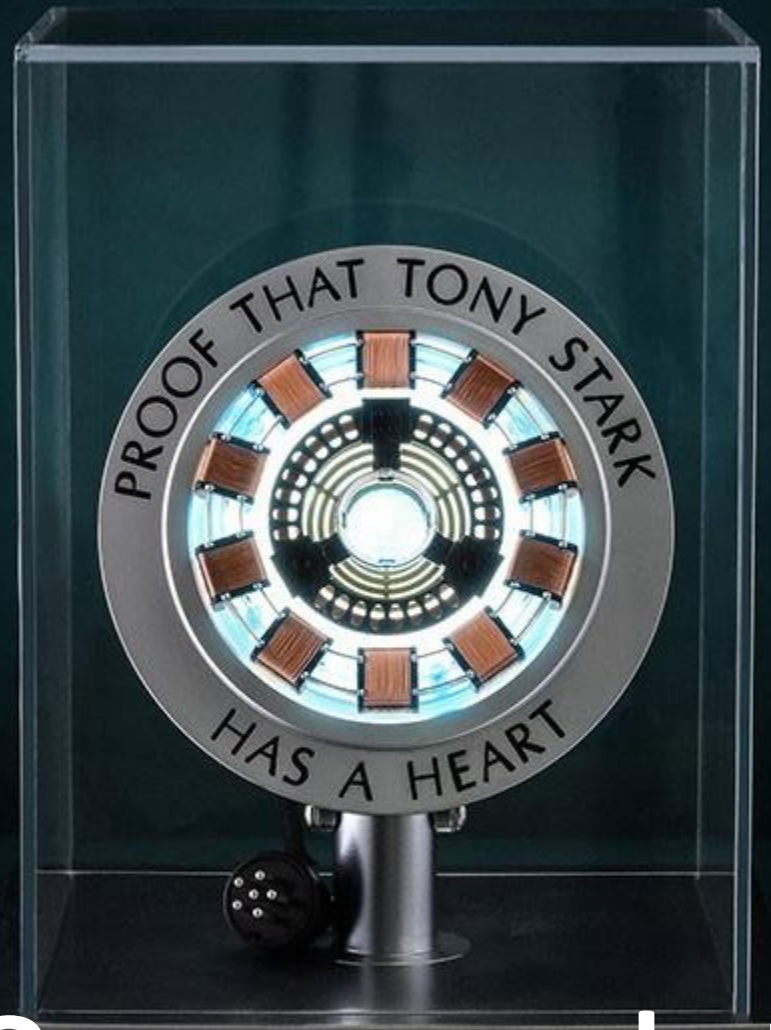


IAST
- Combine dynamic/static
- Good false positives/negatives
- Immature but getting there



THE BEST TOOL IS…

Pero como Tony Stark



DevSecOps Tiene un corazón

DevSecOps no es solo tooling……

CALMS (El guantelete del loop infinito)

CSA LATAM FORUM 2019

Culture

Automation

Lean

Measurement

Sharing



Originalmente acuñado CAMS por John Willis y Damon Edwards después del primer evento DevOpsDays con sede en EE. UU. Celebrado en Mountainview California en 2010, . Jez Humble luego agregó la L, para Lean, haciéndolo CALMS.

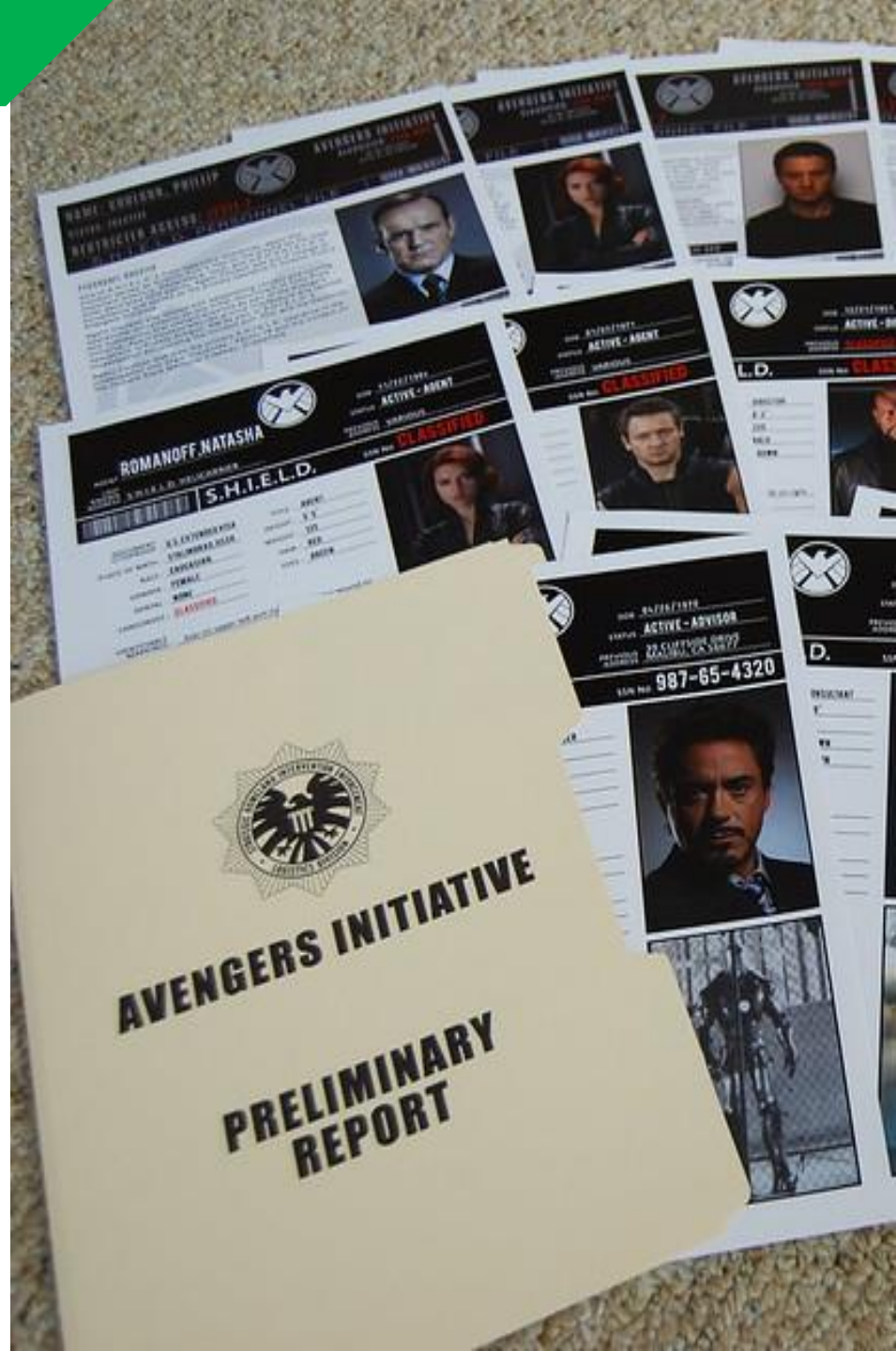
Culture

¿Por qué la cultura es crítica?

DevSecOps es el principio de que todos los equipos de tecnología son responsables de la ciberseguridad en una organización: la propiedad no está únicamente en manos de los profesionales y equipos de seguridad.

La idea de que la ciberseguridad es tarea de todos se debe en parte a que las competencias en materia de ciberseguridad están limitadas dentro del mercado en su conjunto y dentro de una organización en particular:

- **La seguridad se considera (y a menudo puede ser) un bloqueador**
- **Prácticas laborales que resultan en conflictos cotidianos.**
- **Traspasos, demoras y costos innecesarios para entregar valor**
- **Incumplimientos que cuestan dinero y daños a la reputación**



Culture

CSA LATAM FORUM 2019



Culture

CSA LATAM FORUM 2019



La limitación se ve exacerbada por el diseño organizacional tradicional que tiene la seguridad como un equipo separado, a veces dos equipos separados (uno de seguridad y otro de InfoSec), a menudo con líneas de reporte equivocado.

Una de las primeras preguntas que solemos hacer a una organización es acerca de su diseño organizacional: tener equipos de seguridad separados crea tensión ("no, no y no"), transferencias y retrasos en el proceso.

Una cultura de DevSecOps se define principalmente, por la alta confianza. Cuando tenemos altos niveles de confianza, hay bajos niveles de fricción y el trabajo puede fluir a alta velocidad, por lo que cuesta menos entregar valor.

Es difícil hablar de cultura, pero más difícil para nosotros los de tecnología, ya que estamos más acostumbrados hablar en bits y bytes que en emociones y sentimientos.



Culture



Para fomentar la confianza, necesitamos crear un lugar de seguridad psicológica, un lugar donde las personas puedan ser sinceras y experimentales sin temor a las consecuencias, especialmente si experimentan una falla (como la pelea de Hulk vs Thanos)

Muchos líderes tradicionales, luchan con esta tolerancia a fallos. Particularmente cuando su trabajo es administrar infraestructura críticas “es entendible que vean una falla como catastrofe.”

Pero hay muchos matices de falla: desde un defecto en una rama de desarrollo detectado durante la integración continua hasta un sistema inactivo durante horas para todos los usuarios globales.

Cuando estamos en una situación, como estamos con seguridad, donde el conocimiento, las habilidades y la experiencia son una limitación: **parte de la solución es mejorar el aprendizaje, no queremos una cultura de la culpa, donde la gente tenga miedo a aprender.**

Culture

Entonces, sabemos lo que tenemos, y sabemos a qué queremos aspirar, aquí algunos consejos sobre cosas prácticas que pueden hacer para influir en el cambio:



Culture

Entonces, sabemos lo que tenemos, y sabemos a qué queremos aspirar, aquí algunos consejos sobre cosas prácticas que pueden hacer para influir en el cambio:

Mala Conducta	Buena Conducta	Actividades para Evolucionar el Comportamiento
Desconfiar el uno del otro	**Confiar los unos en los otros**	Capacitar a los líderes para que sean entrenadores, proporcionar plataformas de colaboración (físicas y virtuales), hacer que el trabajo sea visible a través de los backlogs y las tablas Kanban
Desconfianza en el proceso	**Confiar en cada proceso**	Usar técnicas como el Mapeo de Flujo de Valor para obtener un entendimiento compartido en el sistema de extremo a extremo.
Temor	**Coraje**	No castigar los errores o experimentos fallidos, sino crear un ambiente de seguridad psicológica y sistemática donde la gente pueda ser valiente y el valor sea recompensado.
Hice mi trabajo	**Responsable**	Trate el fracaso como una oportunidad de aprendizaje y pregunte a la gente sobre el descubrimiento y la remediación no ponga más controles. Utilice el mapeo de flujos de valor para avanzar en la responsabilidad compartida
Reactivo	**Reflexivo**	No cierre un incidente hasta que se haya completado un experimento con una hipótesis exitosa para la remediación. Demasiadas organizaciones me dicen que sólo tienen tiempo para arreglar el problema, no para reflexionar sobre él.
Estática	**Estudiantes**	Ayudar a las personas a desaprender los comportamientos existentes y a utilizar la formación y el aprendizaje experimental y ayudar a las personas a comprender el desaprendizaje, la neuroplasticidad, la práctica y la automaticidad.


La cultura se come a la estrategia... en el desayuno
Peter Drucker

Automation

¿por qué necesitamos automatización?

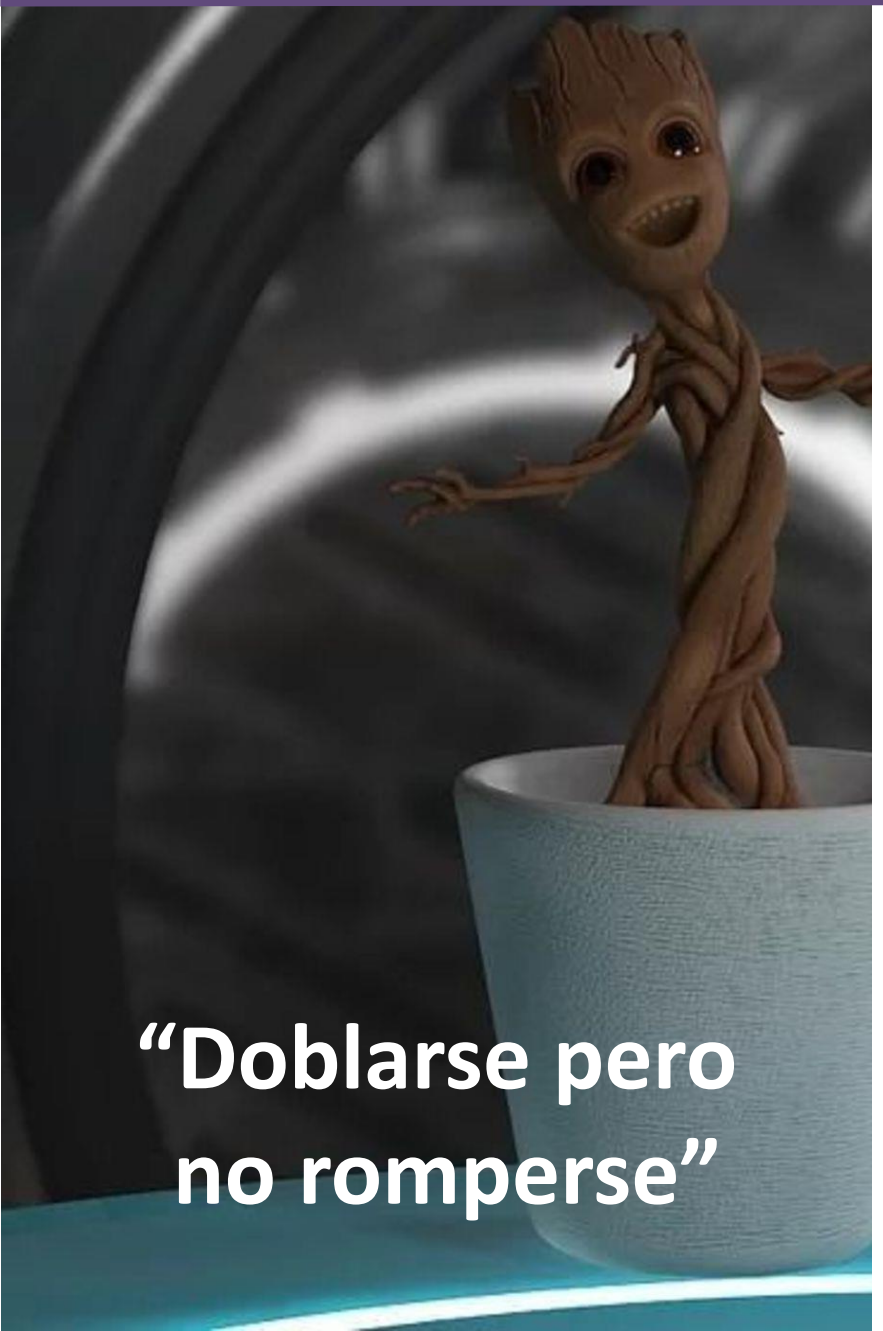
"La automatización es para DevSecOps, como el walkman para Star-Lord".

Esta frase nos deja a Guardianes de Galaxia para esta analogía.

- Las estrellas, serian los clientes que estamos mirando o los resultados de valor que queremos ofrecerles.
- Los Guardianes somos nosotros, los practicantes de DevSecOps.
- El planeta en el que nos encontramos es nuestra organización;
- Los otros planetas son nuestros socios y competidores.
- Los meteoritos son amenazas e incidentes con los que tenemos que lidiar.
- Los telescopios son esenciales para permitirnos ver, recopilar datos y retroalimentación y acelerar la entrega del cambio.



Automation



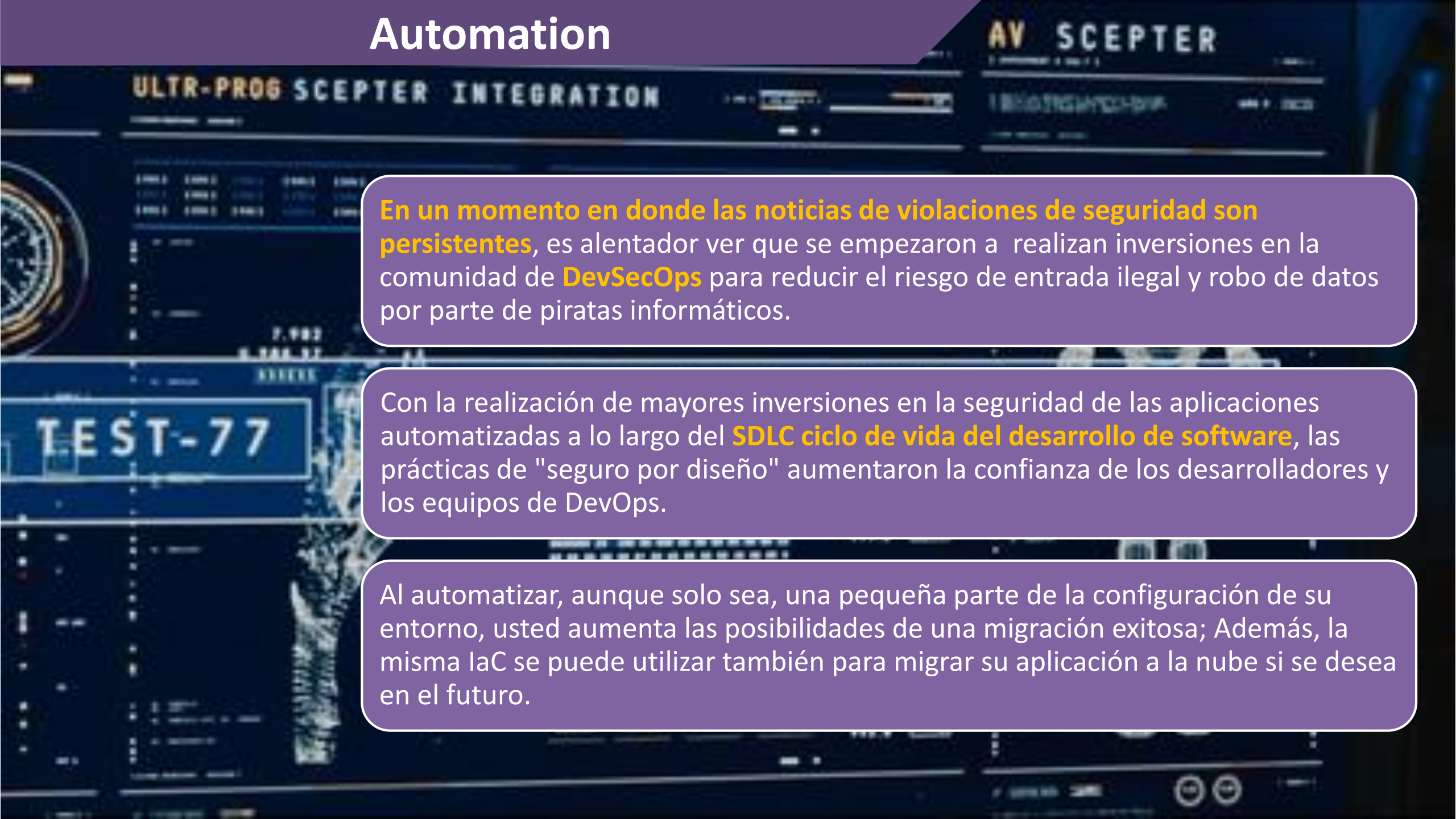
CSA LATAM FORUM 2019

Pero no podemos, y no debemos, tratar de automatizar todo en la vida. Pasará bastante tiempo antes de que todos podamos ir a tumbarnos en la playa, mientras las máquinas hacen todo el trabajo….

Pero podemos **AUTOMATIZAR** para dejar de hacer **TRABAJOS REPETITIVOS Y ABURRIDOS** y romper las restricciones que vemos en nuestro trabajo: la seguridad, que es una de las restricciones clave cuando pensamos en proyectos Agiles.

Todo esto se debe considerar en el contexto de la entrega continua (CD), es decir, la práctica de tener siempre el software en un estado liberable y seguro.

Automation



En un momento en donde las noticias de violaciones de seguridad son persistentes, es alentador ver que se empezaron a realizan inversiones en la comunidad de **DevSecOps** para reducir el riesgo de entrada ilegal y robo de datos por parte de piratas informáticos.

Con la realización de mayores inversiones en la seguridad de las aplicaciones automatizadas a lo largo del **SDLC ciclo de vida del desarrollo de software**, las prácticas de "seguro por diseño" aumentaron la confianza de los desarrolladores y los equipos de DevOps.

Al automatizar, aunque solo sea, una pequeña parte de la configuración de su entorno, usted aumenta las posibilidades de una migración exitosa; Además, la misma IaC se puede utilizar también para migrar su aplicación a la nube si se desea en el futuro.

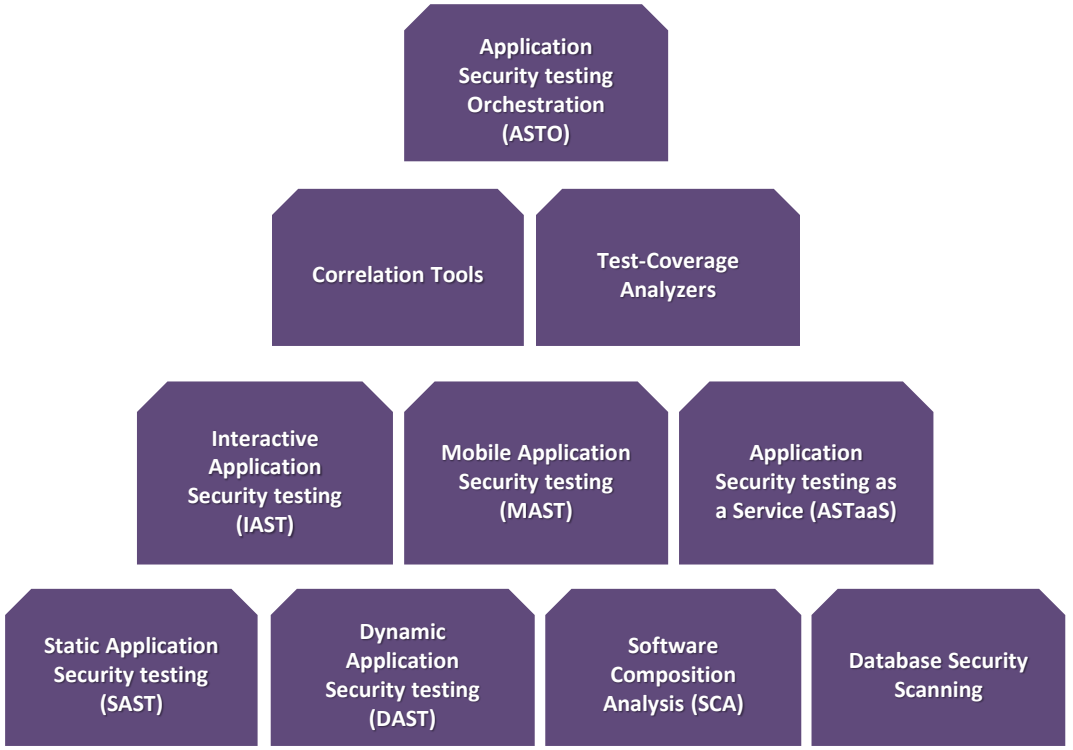
Automation

CSA LATAM FORUM 2019

Esta pirámide representa clases o categorías de Application Security testing tools .

Los límites se difuminan a veces, ya que determinados productos podrían realizar elementos de varias categorías, pero son aproximadamente las clases de herramientas dentro de este dominio.

Hay una jerarquía áspera en que las herramientas en la parte inferior de la pirámide son fundacional y como la competencia se gana con ellos, las organizaciones podrían buscar utilizar algunos de los métodos más progresivos más altos en la pirámide





https://cloudlegion.com.ar/blog/201901.html



CSA LATAM FORUM 2019

Aunque Seguro estén pensando lo mismo que Thanos, que pueden eliminar la mitad de su equipo de pentest, eso no es así….

El equipo actual evoluciona y se focaliza en agregar valor, buscando posibles fraudes o riesgos potencialmente reales y no solo correr herramientas….

CSA LATAM FORUM 2019

¿Cómo Lean mejora el rendimiento?

Se trata fundamentalmente de crear una cultura de aprendizaje. Esto está en contraste con la naturaleza prescriptiva y muy planificada del pasado en seguridad.

En lugar de tratar de reunir todos los requisitos y comprender todos los casos de uso, y luego decirle a la gente qué hacer, aprendemos a medida que avanzamos.

DevSecOps ya nace tomando la cultura de aprendizaje, invitando explícitamente a seguridad al juego de ofrecer valor al cliente más rápido.

En la era del **"Time to Market"** la seguridad ya no puede mantenerse en secreto y ser vista como una barrera para la entrega, sino que debe adoptar la **automatización, el aprendizaje, la medición, el intercambio y aprender a convertirse en un acelerador**.

Podemos lean aplicado en "MARK"



Lean



CSA LATAM FORUM 2019

Existen varias herramientas de **DevSecOps** que pueden ayudar con la implementación de "**LEAN**" una de ellas es **TaskTop**. Estas tools ayudan en la optimización del flujo de la idea a la realización, un marco de conectividad que le quita el dolor de escribir y gestionar las integraciones y visualizar los tiempos de espera y los ciclos. nos muestra dónde están los cuellos de botella.

En nuestra experiencia recomendamos ejecutar **Value Stream Mapping**, como parte de su viaje a **Lean** ya que brinda métricas increíblemente poderosas, pero difiere de TaskTop en que no es manejado por datos sino por las ideas de la gente.

No es que esto sea necesariamente bueno o malo, pero una combinación de hombre y máquina puede funcionar mejor en el clima de negocios que tenemos hoy en día.

"Los seres humanos todavía necesitan interpretar las tendencias y, en su mayoría, decidir cómo actuar sobre la base de lo que los datos les dicen. Y a menudo los datos aún no están disponibles."

Lean



Podemos adoptar **Kanban,** es tan poderosa en parte porque se trata de visibilidad, y la visibilidad construye confianza nutriendo a DevSecOps.

Kanban puede ayudar a mostrar dónde están los bloqueadores y dónde tenemos demasiado trabajo en curso. Fundamental para impulsar las conversaciones sobre la mejora.



Foco en la mejora, recomendamos a todas las organizaciones a que se vuelvan experimentales para impulsar la innovación al tiempo que reducen el riesgo.

El uso del **"kata"** de mejoras de lean es clave para que esto se convierta en algo habitual, alejándose de una cultura de reuniones y planificación, hacia pequeñas y frecuentes mejoras incrementales.

Lean

Esta idea de mejora incremental y continua también se refleja en el **Kaizen for DevOps**, un modelo que nos lleva a animar a nuestros clientes a pensar en un viaje de DevOps en términos evolutivos y no transformacionales, alcanzando un estado general de mejora más rápido.

Dado que el impacto de los cambios más pequeños en la productividad es menor y el sistema organizativo tiene tiempo para recuperarse más rápido y hacer otro cambio pequeño más rápido.

"Un incidente es una inversión no planificada, y si no lo ves de esa manera como un líder, no estás obteniendo un retorno de la inversión que ya se hizo en tu nombre".

Sin embargo, no nos sentimos a menudo de esta manera, especialmente en el caso de las violaciones de seguridad. Pero esto nos lleva a otro concepto lean: el Andon Cord y su relación con la cultura organizacional de alta confianza.





https://www.developer.com/mgmt/a-kaizen-approach-for-devops-how-to-help-teams-find-and-fix-their-own-problems.html

Lean

CSA LATAM FORUM 2019

Necesitas una cultura que estimule y recompense a los empleados a pensar como **intra-emprendedores**.

- Imagina que Sony no le hubiera dejado a Ken Kutaragi trabajar en su idea...
- O que Google no dejara que Paul Buchheit trabajara en su idea...

En 1975, un empleado de Kodak inventó la cámara digital. Sus jefes le hicieron esconderla.

¿Qué camino queremos seguir?

NETFLIX

BLOCKBUSTER

Measurement

Medición para ahorrar tiempo y evitar infracciones

Vimos que **lean** se preocupa por identificar y eliminar los errores de la línea de producción, por lo que la métrica que más asociamos con ella es el tiempo total del ciclo.

Es super eficaz para mostrarnos cuándo nuestro modelo de seguridad está actuando como un cuello de botella, pero ¿qué otras medidas son útiles en el mundo de DevSecOps?

Esencialmente, queremos resultados de valor en las manos de nuestros clientes lo más rápido posible y este es el elemento clave de un caso de negocios de DevSecOps, sin comprometer al mismo tiempo la integridad del sistema, rendimiento y estabilidad.



Measurement

CSA LATAM FORUM 2019

En **DevSecOps** queremos seguridad incrustada en el pipeline del flujo de valor. Eso significa que:

- Los requisitos de seguridad (NFRs) están incorporados en el backlog de desarrollo.
- No se pierde tiempo esperando aprobaciones o las pruebas de seguridad durante el desarrollo.
- Las pruebas de seguridad están integradas en el pipeline de CI/CD
- Las pruebas de seguridad no requieren contacto ni tiempo de espera
- Las acciones IT Ops/Sec Ops están disponibles como autoservicios homologados para los DEVs



Si seguimos este patrón significa que la seguridad no representa desperdicio en el flujo de valor, por lo que el tiempo de ciclo se optimiza desde esta perspectiva.

Measurement

CSA LATAM FORUM 2019

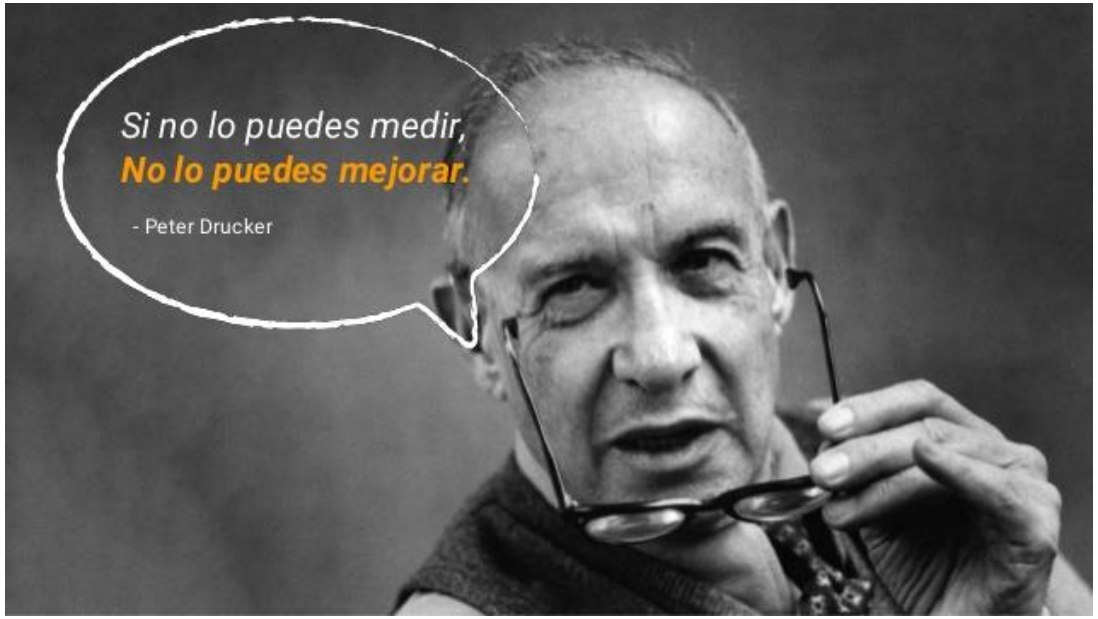
DevSecOps no es otra cosa que, un conjunto de patrones de formas de trabajo que mejoran el desempeño organizacional.

Entonces, ¿cómo medimos la eficacia de DevSecOps y la entrega de valor? ¿Cómo determinamos cuándo DevSecOps ya no es una 'cosa' ?

Existen innumerables métricas posibles en una plataforma DevSecOps. La decisión de qué métricas seguir se basa en gran medida en las necesidades del negocio y en los requisitos de cumplimiento.
Para facilitar esta visión podemos verlas en dos grupos:

Métricas de alto valor

Métricas de apoyo



Measurement

CSA LATAM FORUM 2019

Métricas de alto valor

Estas métricas deben implementarse primero en una nueva plataforma. No todas las plataformas tendrán estas métricas disponibles de inmediato, pero un entorno completamente maduro generalmente tendrá todas estas métricas disponibles.

Métrica	Descripción
Frecuencia de implementación	Número de implementaciones en producción en un período de tiempo determinado
Cambiar el tiempo de entrega (para aplicaciones)	Tiempo entre una confirmación de código y la implementación de producción de ese código
Cambiar volumen (para aplicaciones)	Número de historias de usuario implementadas en un período de tiempo determinado
Cambiar tasa de falla	Porcentaje de despliegues de producción que fallaron
Tiempo medio de recuperación (MTTR) (para aplicaciones)	Tiempo entre un despliegue de producción fallido hasta la restauración completa de las operaciones de producción.
Disponibilidad	Cantidad de tiempo de actividad / tiempo de inactividad en un período de tiempo determinado, de acuerdo con el SLA
Volumen de problemas del cliente	Número de problemas reportados por los clientes en un período de tiempo determinado
Tiempo de resolución de problemas del cliente	Tiempo medio para resolver un problema informado por el cliente
Tiempo para valorar	Tiempo entre una solicitud de función (creación de la historia del usuario) y la realización del valor comercial de esa función
Hora de ATO	Tiempo entre el comienzo de Sprint 0 para lograr un ATO
Hora de parchear vulnerabilidades	Tiempo entre la identificación de una vulnerabilidad en la plataforma o aplicación y la implementación exitosa de la producción de un parche

Measurement



Métricas de apoyo

Estas métricas proporcionan información útil y se recomienda que las métricas en esta categoría se implementen después de que se hayan implementado las métricas de alto valor.

Métrica	Descripción
Prueba de cobertura	Porcentaje de código cubierto por pruebas automatizadas
Cambiar tipos	Porcentaje de características frente a correcciones frente a parches de seguridad
Tiempo de disponibilidad de información del evento.	Tiempo desde un evento hasta información sobre el evento que está disponible para el equipo DevSecOps o los usuarios finales
Incorporación de desarrolladores	Tiempo desde que un desarrollador se une al equipo hasta la capacidad de confirmar el código para la implementación de producción
Cambiar tiempo de resolución	Tiempo entre una propuesta de cambio y el cierre (implementación o rechazo)
Cambiar el tiempo de entrega (para la plataforma DevSecOps)	Tiempo entre un cambio (por ejemplo, confirmación de código) y la implementación de la plataforma de ese cambio
Cambiar volumen (para la plataforma DevSecOps)	Número de historias de usuario implementadas en un período de tiempo determinado
Cambiar la tasa de falla (para la plataforma DevSecOps)	Porcentaje de despliegues de plataforma que fallaron
Tiempo medio de recuperación (MTTR) (para la plataforma DevSecOps)	Tiempo desde un despliegue fallido de la plataforma hasta la restauración completa de las operaciones de la plataforma
Cambiar el tiempo de entrega de las imágenes	Tiempo desde la identificación de la necesidad de una imagen nueva / actualizada hasta su disponibilidad para uso en producción
Frecuencia de publicación de imágenes	Número de imágenes nuevas / actualizadas publicadas en un período de tiempo determinado
Disponibilidad de registro	Cantidad de tiempo de actividad / tiempo de inactividad del sistema de registro en un período de tiempo determinado
Número de alertas de monitoreo	Cantidad de alertas de monitoreo activadas en un período de tiempo determinado
Número de pruebas de unidad / integración	Número de unidades automatizadas o pruebas de integración para una aplicación.
Número de pruebas funcionales / de aceptación.	Número de pruebas funcionales o de aceptación automatizadas para una aplicación
Punto de recuperación medio	Rango de tiempo medio de datos que se pierden debido a un incidente
Cumplimiento de control de retención	Porcentaje de controles relacionados con la retención (por ejemplo, AU-11, SI-12) que están automatizados
Instanciación de imagen	Tiempo transcurrido entre el momento en que un desarrollador solicita la creación de instancias de imagen y su creación de instancias real

Measurement

CSA LATAM FORUM 2019

Métricas de apoyo

Métrico	Descripción
Desviación de referencia de seguridad	Desviación entre los puntos de referencia de seguridad aplicados a una imagen y los puntos de referencia de seguridad en una imagen instanciada
Controles técnicos	Número de controles técnicos de seguridad implementados parcial o totalmente
Frecuencia de parches de vulnerabilidad	Con qué frecuencia los parches de vulnerabilidad se implementan regularmente en producción
Tiempo de entrega de parches de vulnerabilidad	Tiempo entre el descubrimiento de una nueva vulnerabilidad (es decir, su publicación) y el parcheo en la producción
A & A tiempo de entrega	Tiempo entre el inicio de una evaluación de cumplimiento de seguridad y la finalización de los procesos de A&A
Los hallazgos de SAR cuentan	Número de hallazgos en el Informe de evaluación de seguridad (SAR)
Recuento de POA y M	Número de POA y Ms
Plazo de entrega de revisión de seguridad de nueva arquitectura	Tiempo transcurrido entre el inicio de una solicitud de revisión de seguridad de una nueva arquitectura y la finalización
Experimentos y alternativas	Número de experimentos tecnológicos y componentes alternativos probados.
Cuenta de registro del sistema	Número de sistemas (aplicaciones, SO, servicios) en una plataforma DevSecOps que están registrando
Cumplimiento de control de seguridad de AU	Lista y porcentaje de controles de seguridad de AU que se satisfacen mediante las prácticas de registro de la plataforma DevSecOps
Plazo de aprobación de CM	Tiempo entre el envío de una solicitud de cambio y su aprobación
Plazo de aprobación de implementación	Tiempo transcurrido entre la solicitud de implementación de un cambio aprobado y la implementación real en producción
Tiempo de entrega de notificaciones	Tiempo entre cualquier paso dado del proceso de MC y la notificación de todas las partes interesadas
Tiempo de entrega de aprovisionamiento de usuarios	Tiempo entre la solicitud de un nuevo usuario en la plataforma y el usuario que puede iniciar sesión
Cumplimiento de control de seguridad de CA	Lista y porcentaje de controles de seguridad de CA que se satisfacen mediante las prácticas de administración de cuentas de la plataforma DevSecOps
Frecuencia de auditoría de privilegios	Número de veces en un período de tiempo determinado que los usuarios y sus privilegios son auditados
Recuento de administrador	Lista y número de usuarios que tienen privilegios de administrador
Frecuencia de rotación secreta	Número de veces en un período de tiempo dado que los secretos se cambian y actualizan cuando se ven afectados
Plazo de incorporación	Tiempo entre una solicitud de una nueva aplicación para usar la plataforma DevSecOps y la aplicación que se está implementando en la plataforma
Tiempo de entrega de gastos	Tiempo entre un gasto y el informe del gasto.

El poder de Dojos y ChatOps en el intercambio de conocimientos de seguridad

En resumen, **DevSecOps** tiene dos impulsores principales: La seguridad es una restricción en la mayoría de las organizaciones y ha sido una ocurrencia tardía en el mundo de DevOps.

“DevOps busca optimizar el flujo de resultados de valor desde la idea hasta la realización mediante la eliminación de cuellos de botella y la amplificación de la retroalimentación”

Como vimos antes podemos abordar esta restricción con las prácticas de automatización, pero también esta el enfoque cultural para abordar este problema también, y todo se centra en el intercambio efectivo de conocimientos.

Un patrón que aconsejamos y que hemos visto que funciona con eficacia en varias ocasiones es que uno o dos miembros de la 'torre de marfil' de seguridad se integren y se ubiquen en el equipo de productos por un período temporal, alrededor de tres meses. funciona bien.

Sharing

CSA LATAM FORUM 2019

La regla 80:20 parece aplicarse aquí; Se necesita el 20% del conocimiento en el 80% de las situaciones, por lo que la cantidad requerida de conocimiento se contagia rápidamente cuando un pequeño grupo de humanos trabaja en estrecha colaboración.

Los expertos en seguridad pueden pasar a más equipos de productos: el conocimiento que habrán adquirido durante este proceso acelerará el intercambio de conocimientos en los nuevos equipos que visiten.

Esto requiere tener seguridad a bordo con la visión de DevOps y necesita algunas personas de mente abierta dispuestas a cambiar sus prácticas de trabajo cotidianas.

El liderazgo tiene que ponerle un sello de goma y tenemos que hacer un intercambio entre **"no podemos encontrar tiempo para ahorrar tiempo"**



Sharing



Estos ágiles, DevOps, defensores de DevSecOps, llámalos como quieras, también pueden ser alentados a hacer otras cosas para ayudar a compartir el conocimiento.

Por ejemplo, podrían comenzar una comunidad DevSecOps de interés / práctica o gremio donde inviten a las personas (cualquier persona interesada) a participar en talleres, reuniones, espacios en línea o incluso hackatones y compartir sus ideas de esa manera.



La mayoría de las organizaciones con las que trabajamos usan algún tipo de wiki, ya sea Confluence o Teams u otra cosa. Sin embargo, un error común en este tipo de plataformas es que se vuelven extensas y difíciles de navegar si no se mantiene en el tiempo.

Sharing

CSA LATAM FORUM 2019

La mayor parte del mundo ágil y DevOps ahora opera en Jira (hay otras herramientas de gestión de pedidos pendientes disponibles, pero esta es la más popular). Y todos saben cómo usar una herramienta de chat grupal (¿tiene WhatsApp, sí?).

Slack es popular en equipos de tecnología, pero Office365 está disponible en casi todas partes. Ambos tienen la capacidad de integrarse con herramientas en la cadena de herramientas DevOps y chat grupal + herramientas = **ChatOps.**

Una plataforma de colaboración genera confianza a través de la visibilidad y puede mejorar los tiempos de recuperación y la estabilidad del sistema.

“Por ejemplo, en lugar de entrar en una sala de guerra y poner a la gente en una línea de conferencia cuando ocurre un incidente, si está usando ChatOps, abrirá un canal y todos se apilarán allí”



DevSecOps – Anti patrones

CSA LATAM FORUM 2019

Recientemente leí en alguna parte que los buenos líderes tienen una lista de **"empezar a hacer"** y una lista de **"dejar de hacer"**. Este concepto está en Good to Great (Collins) pero también lo he leído en otros lugares.

La lista **'Dejar de hacer'** normalmente comprende las cosas que no agregan valor o probablemente más importantemente 'interfieren' con el trabajo que agrega valor. Los he escuchado como antipatrones.

De manera similar, DevOps / DevSecOps tienen antipatrones, cosas que destruyen los poderes de DevOps / DevSecOps en las organizaciones.



Patrón



Antipatron

DevSecOps – Anti patrones



- **DevOps / DevSecOps es un proceso/metodología :** No lo es, es una filosofía, una forma de pensar.
- **Agile es igual a DevOps / DevSecOps:** No lo es, es un habilitador que permite flujo de trabajo continuo
- **Cambio de nombre:** Cambiar el nombre de un equipo o nombrar ingenieros con DevOps no significa que seas DevOps.
- **Iniciar un grupo DevOps separado:** Creó otro silo, ¿verdad?
- **La adquisición hostil:** Desarrollo no se hace cargo de las operaciones. Hay una parte igual de responsabilidad entre los equipos de desarrollo y Operaciones.
- **DevOps / DevSecOps es una palabra de moda:** En realidad, algunas personas usan esto como una palabrota ... "¿Puedes hacer esto de una manera DevOps?", Es decir, ¿puedes hacerlo rápidamente y romper las reglas mientras estás en ello? Pienso que es un estado mental y está respaldado por la excelencia en ingeniería.
- **Venden DevOps / DevSecOps como una bala de plata:** Algunas personas piensan que poner estas palabras en la misma oración es como poner 'Queso' y ‘Dulce' en la misma palabra, no lo es, es una de las cosas más difíciles que intentarán y es algo que una organización debe hacer por sí misma con la tutoría y educación adecuadas.

DevSecOps – Anti patrones



- **DevOps significa que los desarrolladores administran la producción:** No, DevOps no asume la responsabilidad de administrar la producción de personas cuya responsabilidad principal es la estabilidad del sistema de producción.
- **DevOps es gestión de lanzamiento impulsada por el desarrollo:** Cualquier cosa que sugiera que DevOps reemplaza las operaciones de TI no tiene sentido. Claro, acelerar y automatizar, pero DevOps no es un proceso o una capacidad de automatización y no es el reemplazo de las operaciones de TI.
- **No podemos hacer DevOps - Somos únicos:** Sí, lo sos, esta es la razón principal por la que DevOps funciona, ya que no es una receta única para todos los cocineros en 5 minutos. Aplica las filosofías y principios y tendrás tu propio sabor DevOps. Una de nuestra frases favoritas es " Usa la cultura para cambiar la cultura "

TO BE CONTINUED...

DevSecOps - Framework



CSA LATAM FORUM 2019

PRE-COMMIT	COMMIT (CI)	ACCEPTANCE (CD)	PRODUCTION	OPERATIONS
THREAT MODELING	STATIC CODE ANALYSIS	INFRASTRUCTURE AS CODE	SECURITY SMOKE TESTS	BLAMELESS POSTMORTEMS
IDE SECURITY PLUGINS	SECURITY UNIT TESTS	CLOUD INFRASTRUCTURE	SECRETS MANAGEMENT	CONTINUOUS MONITORING
PRE-COMMIT HOOKS	CONTAINER SECURITY	DYNAMIC SECURITY TESTS	SECURITY CONFIGURATION	PENETRATION TESTING
PEER CODE REVIEWS	DEPENDENCY MANAGEMENT	SECURITY ACCEPTANCE TESTS	SERVER HARDENING	THREAT INTELLIGENCE

Thank You

ευχαριστώ Salamat Po متشكرم شكراً Grazie

благодаря ありがとうございます Kiitos Teşekkürler 谢谢

ขอบคุณครับ Obrigado شكريه Terima Kasih Dziękuję

Hvala Köszönöm Tak Dank u wel дякую Tack

Mulţumesc спасибо Danke Cám ơn Gracias

多謝晒 Ďakujem תודה நன்றி Děkuji 감사합니다

CLOUD LEGION

