



Microsoft®
Most Valuable
Professional

#GlobalAzure
#AzureDevOps

DEVSECOPS EN AZURE DEVOPS

Christian Ibiri



<https://twitter.com/Christianibiri>



<https://www.linkedin.com/in/christian-ibiri/>

Luciano Moreira da Cruz



https://twitter.com/Luciano_m_cruz



<https://www.linkedin.com/in/lucianomoreiradacruz/>

Antes de empezar con Azure DevOps:

¿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 Operations (DevOps)

DV Trading LLC

Chicago, Illinois

...DevOps engineer to lead 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...

NO!

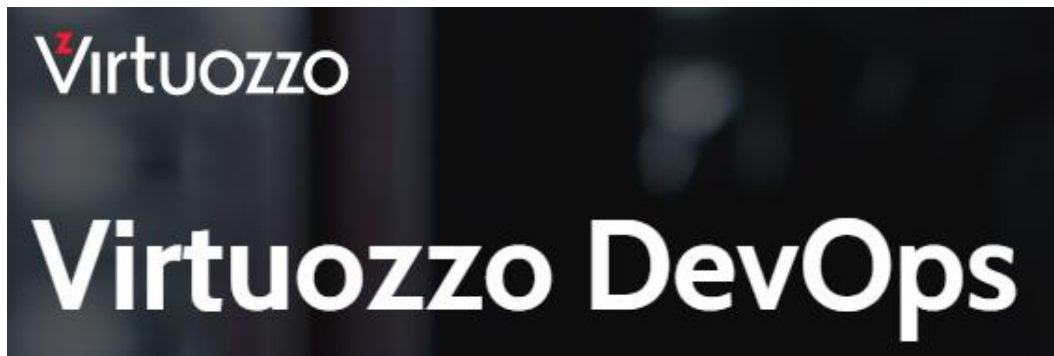
DevOps es un producto?



[Products & Solutions](#) [Industries & Roles](#) [Training & Services](#) [Partners & Developers](#)

Application Deployment and DevOps Tools

DevOps tools to radically shorten application release cycles



DevOps es un producto?



Products & Solutions

Industries & Roles

Training & Services

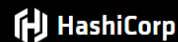
Partners & Developers

Application
Deployment and
DevOps Tools

DevOps tool radically shorten application release cycles

Virtuozzo

Virtuozzo DevOps



DevOps Delivered

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).
- **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. utilizan especialmente herramientas de automatización 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.

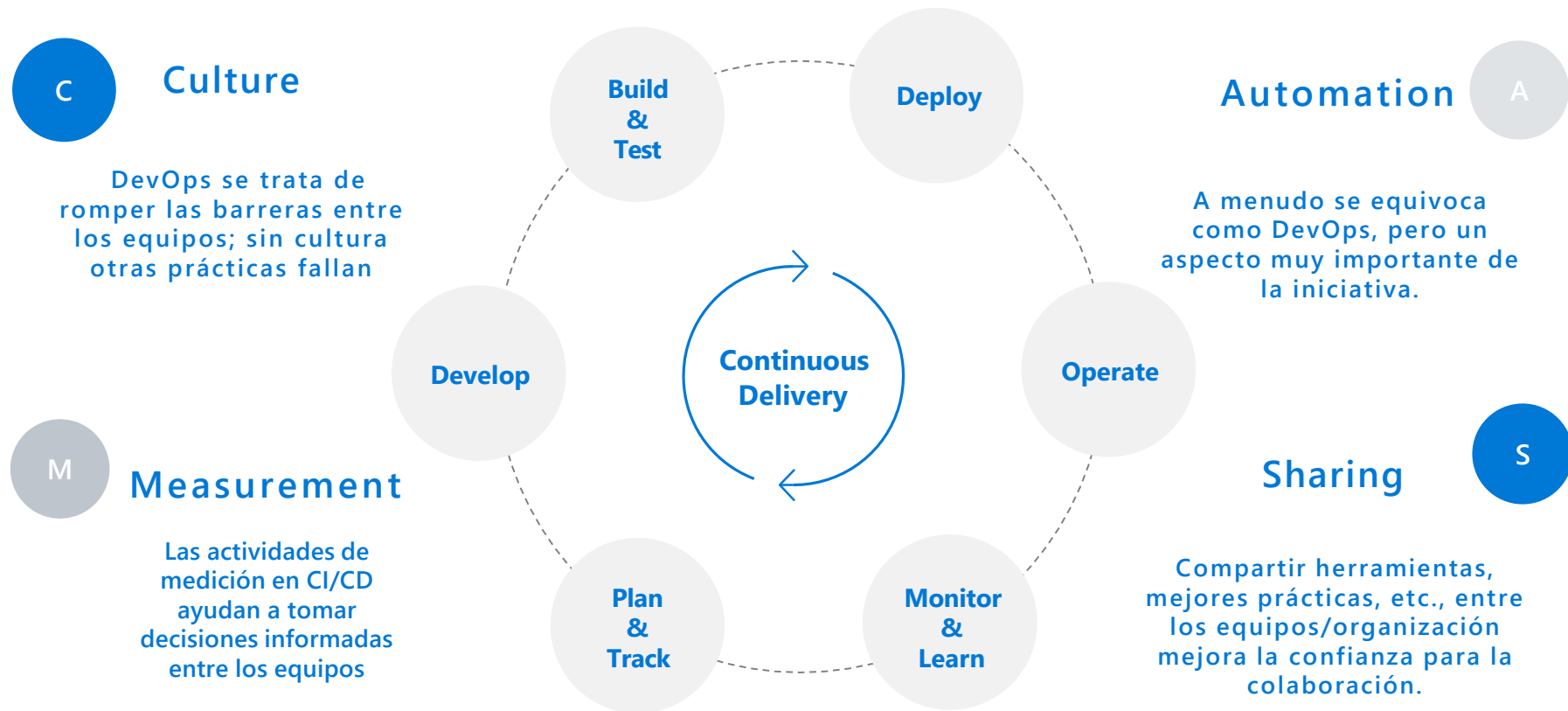
¿Cómo empezó todo?

- 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. Nace 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 DevOps es....



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

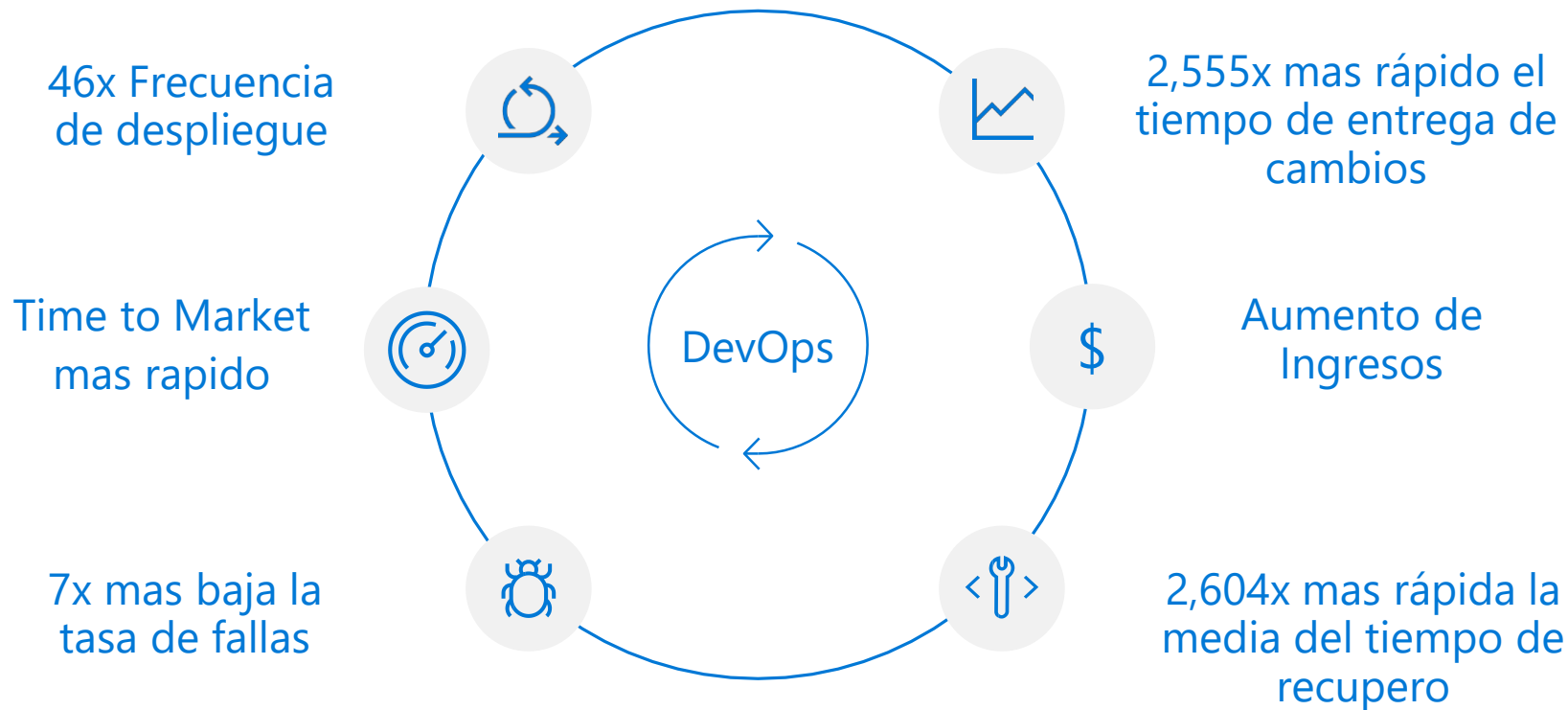


No hay ningún equipo de DEV
No hay ningún equipo de OPS
No hay equipo de SEC
No hay una organización central que "Ejecute" el negocio

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

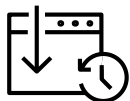


Con DevOps las empresas logran un alto rendimiento...



¿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, puedes entregar software de forma más rápida y fiable, sin importar cuán grande sea tu departamento de IT o qué herramientas estas utilizando.



Integración 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, puedes automatizar todo el proceso desde código hasta la aplicación desplegada en producción.



Aprendizaje automatico y metricas

- Con Azure Application Insights, puedes 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.

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, prueba 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

Obtiene 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.

#AzureDevOps



[@AzureDevOps](https://twitter.com/AzureDevOps)



<https://aka.ms/devopsblog/>

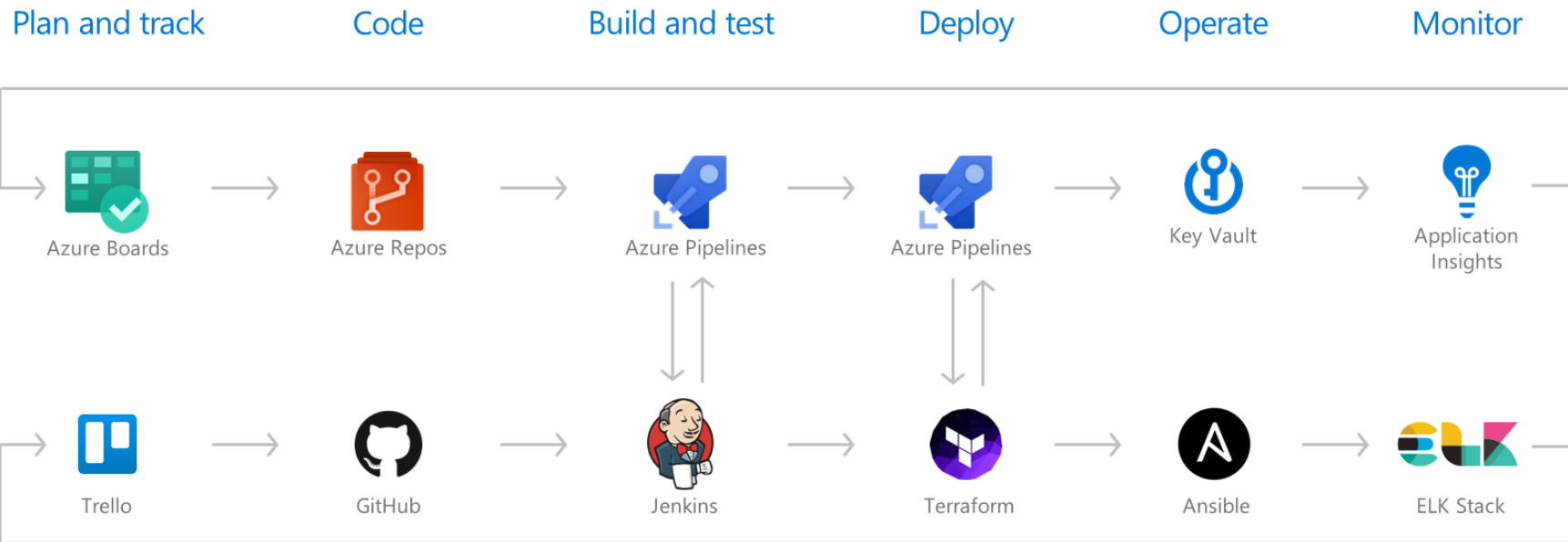


<https://azure.com/devops>



<https://aka.ms/azuredevopsforum>

Azure DevOps vs un pipeline típico



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.microsoft.com/services/devops/pipelines/>

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.microsoft.com/services/devops/boards/>

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/services/devops/repos/>

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/services/devops/test-plans/>

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/services/devops/artifacts/>

Application Insights

Es un **servicio de análisis extensible que supervisa su aplicación activa**. Le ayuda a detectar y a diagnosticar problemas de rendimiento y a comprender qué hacen los usuarios realmente con su aplicación.



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

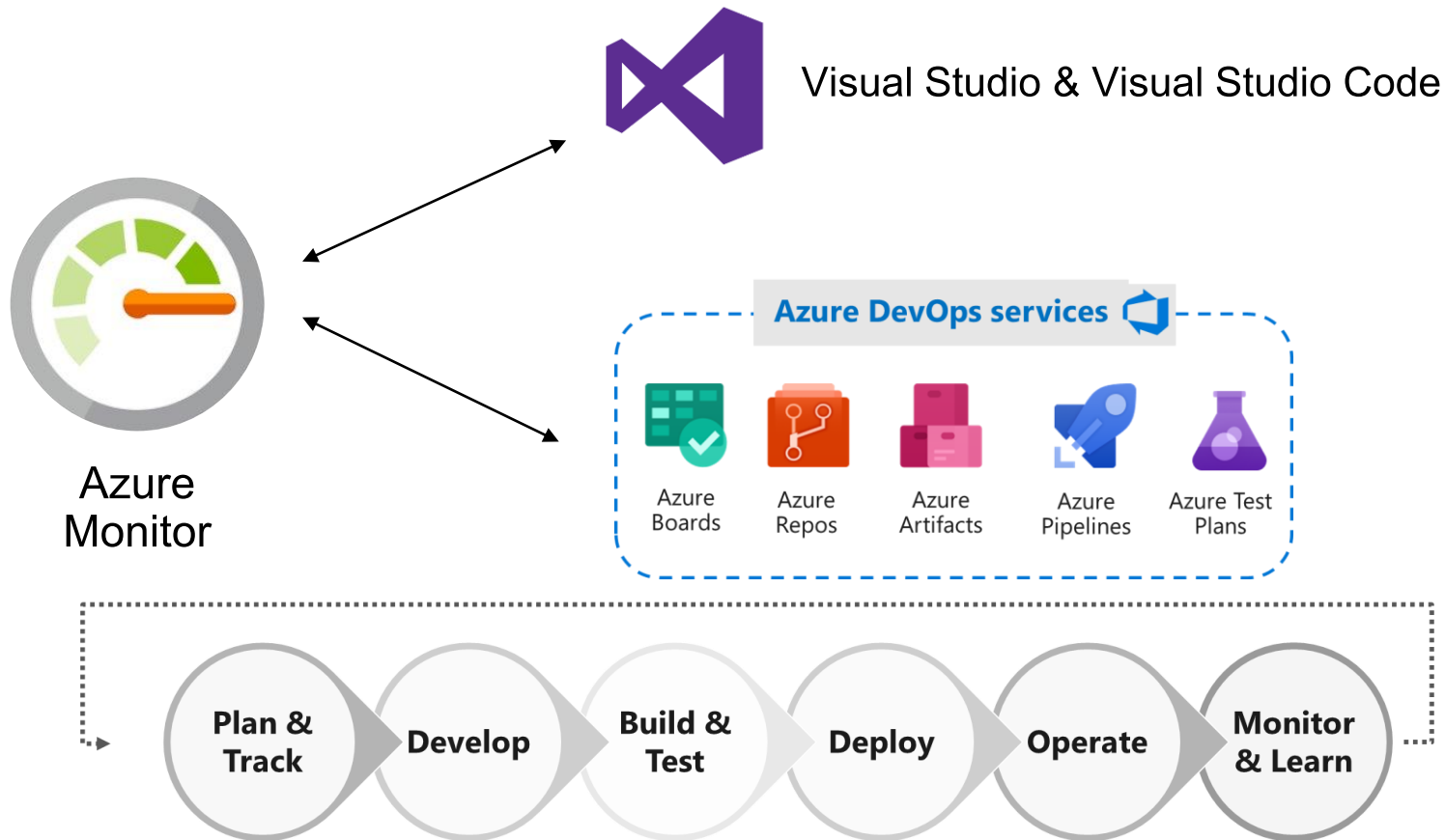


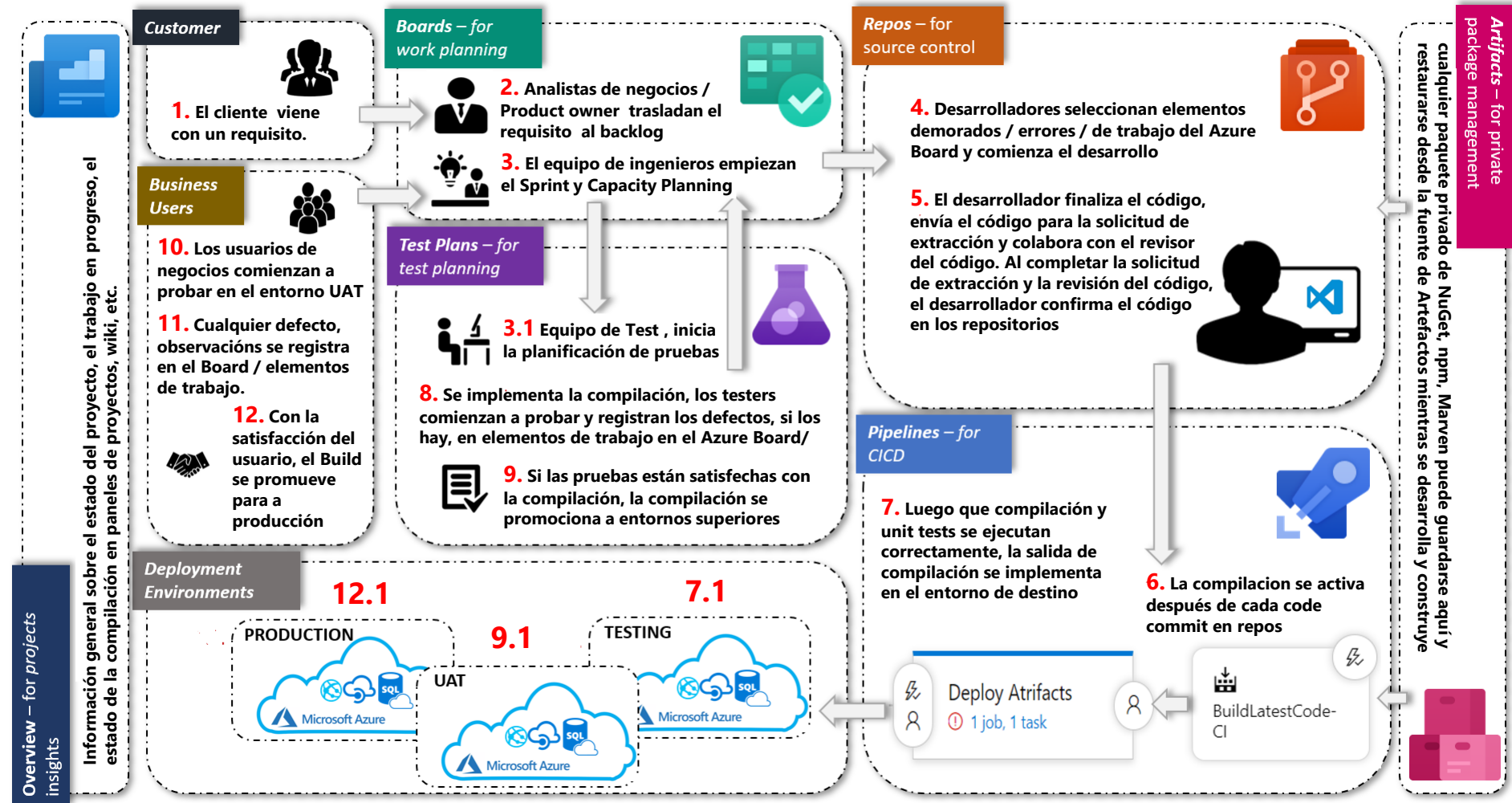
Comprender las cohortes, el comportamiento y el compromiso del usuario final para la planificación.



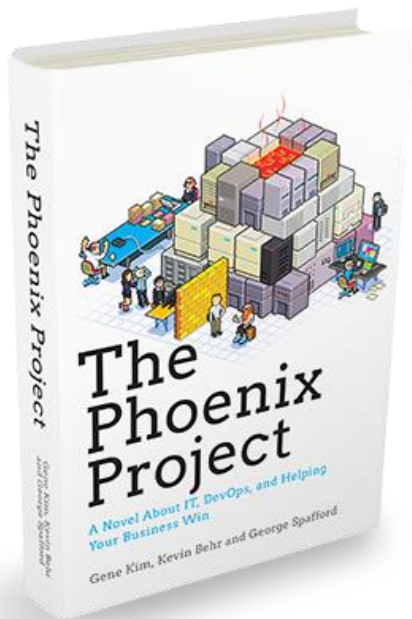
<https://azure.com/services/monitor/>

Monitoreo Continuo (CM) para DevOps y mas..





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

Antes de empezar:

¿Que es DevSecOps?



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:
Descubre las vulnerabilidades
tarde (En Producción)”**



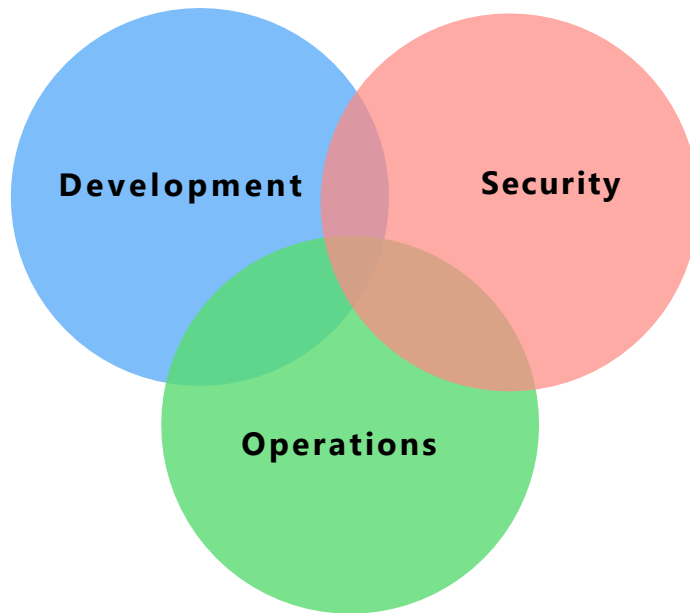
**“Seguridad Tradicional: Les
cuesta mucho acercarse al
equipo de DEV / DEVOPS”**



Como resolvemos eso?

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

Varios nombres para lo mismo:



“DevSecOps”

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

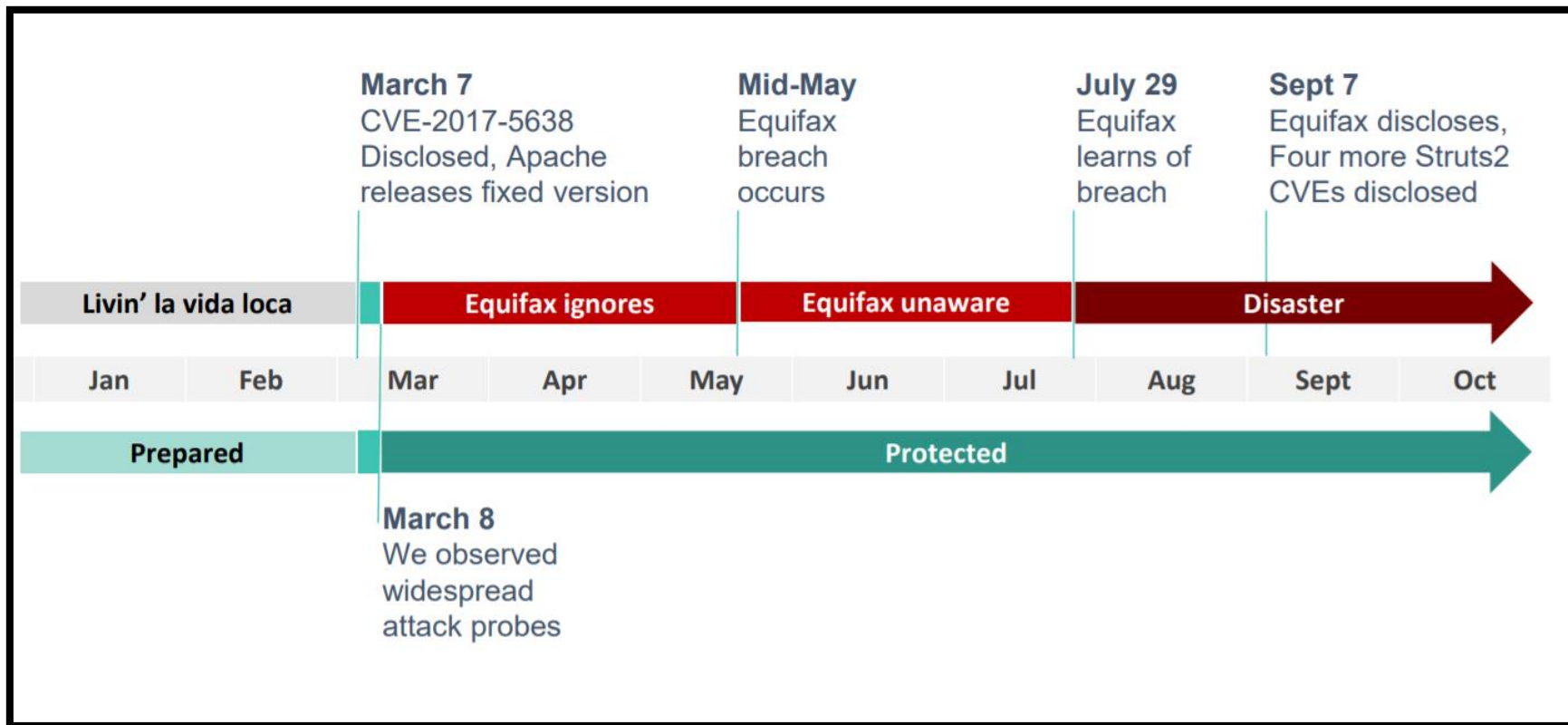
Shared Threat Intelligence over Keeping Info to Ourselves

Compliance Operations over Clipboards & Checklists



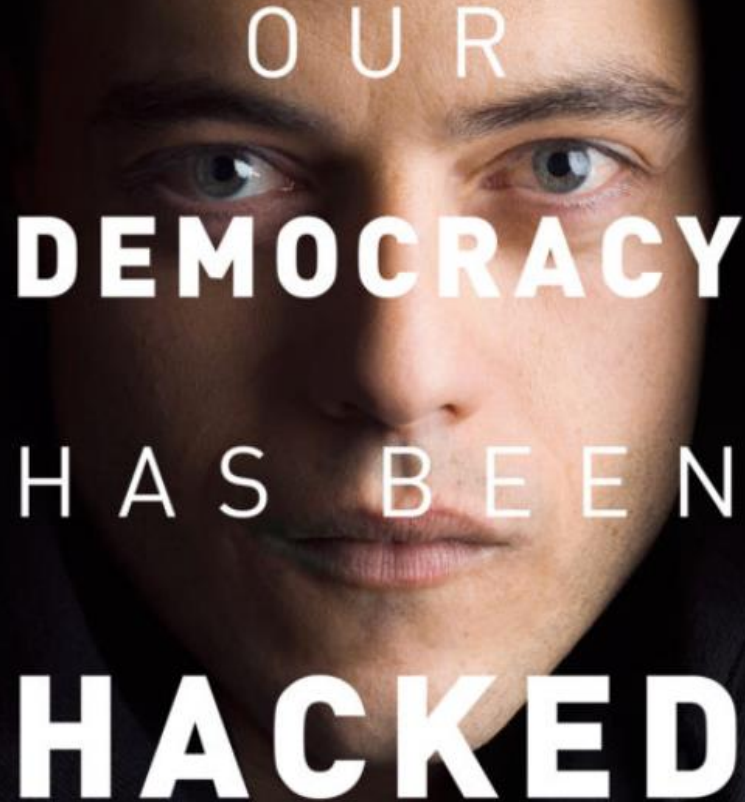
<http://www.devsecops.org/>

¿Por qué?



¿Por qué?

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



OUR
DEMOCRACY
HAS BEEN
HACKED

¿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



Oops, 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 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 do not have 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



Send \$300 worth of bitcoin to this address:

12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

Copy

Check Payment

Decrypt

Uber hack: EU data protection bods launch taskforce

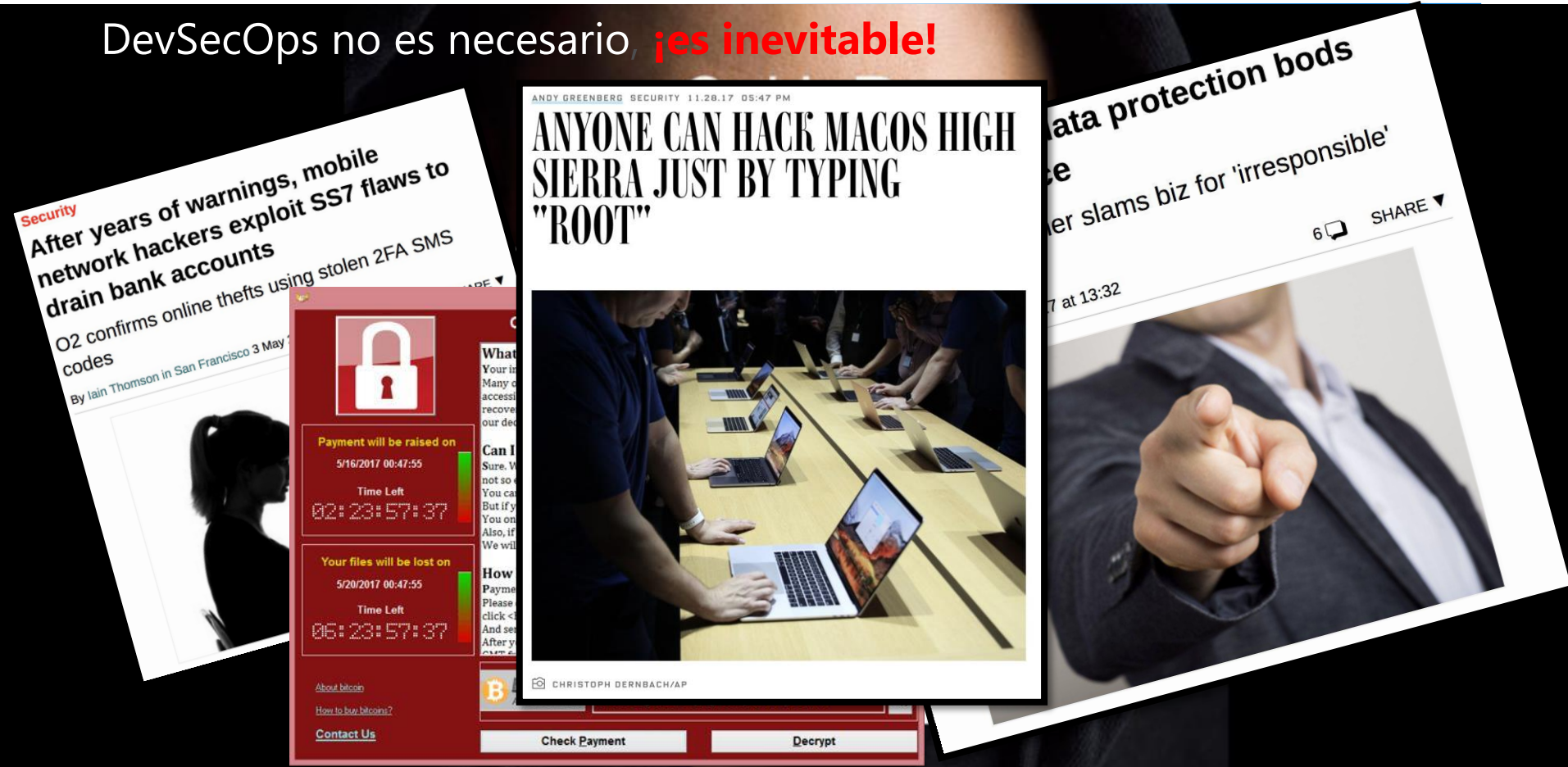
Justice commissioner slams biz for 'irresponsible' behaviour

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!**

ANDY GREENBERG SECURITY 11.28.17 05:47 PM

ANYONE CAN HACK MACOS HIGH

TYPING

ata protection bods

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

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

[How to buy Bitcoin?](#)

[Contact Us](#)

Check Payment

Decrypt

¿Por qué?

DevSecOps no es necesario, ¡es inevitable!

Fuga masiva de datos en Gearbest: cambia ya tu contraseña

15 de marzo, 2019



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.

Contact Us

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 imitada 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.

Check Payment

PM

CK MA
TYPI



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 "Collection #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



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

¿Por qué?

DevSecOps no es necesario, ¡es inevitable!

Fuga masiva de datos en Gearbest: cambia ya tu contraseña

15 de marzo, 2019



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.

Contact Us

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 imitada 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.

Check Payment

PM

CK MA
TYPI



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 "Collection #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.

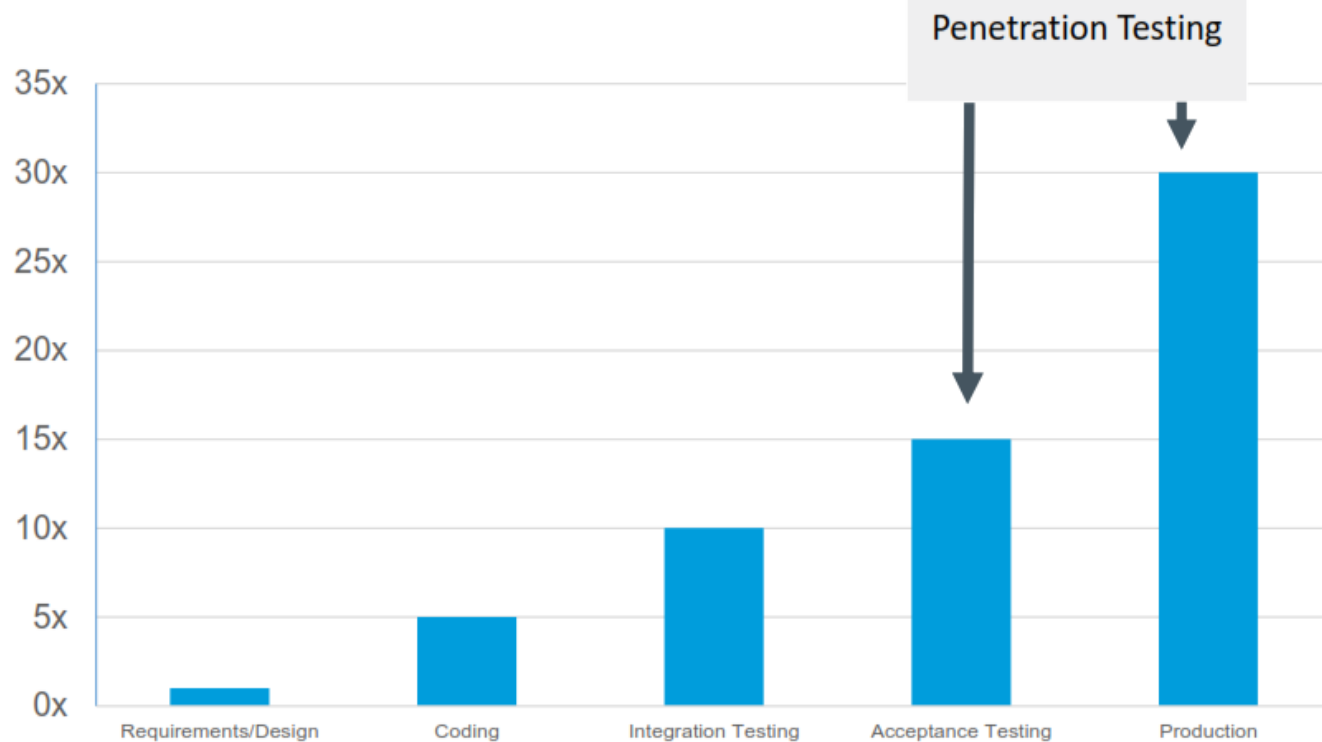
tió la información de 30 millones



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

¿Por qué?

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



■ Relative Cost to fix, based on time of...

¿Por qué?

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

COST OF A DATA BREACH

Sensitive Data Continues to Exit Companies and Cost Millions

Global data breach costs climbed slightly last year



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

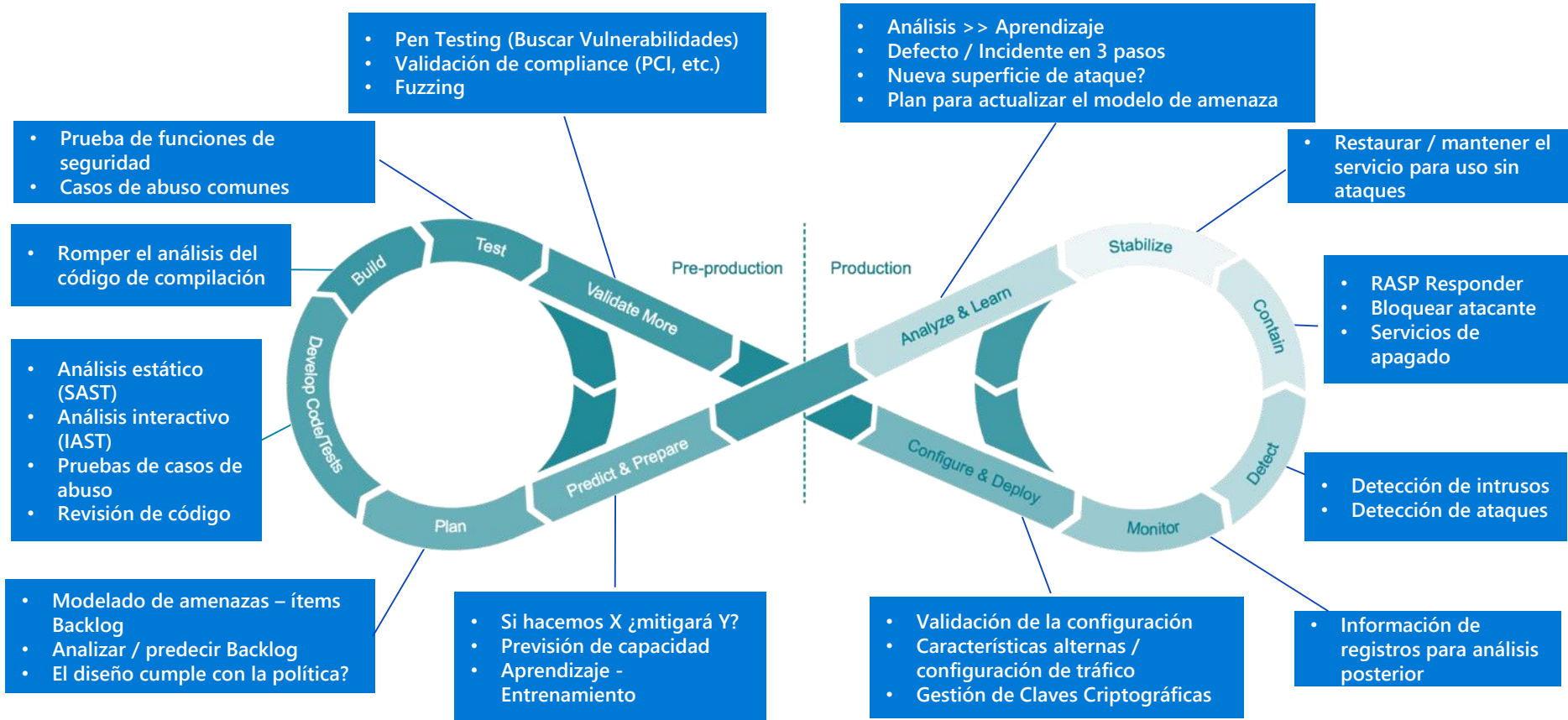
that's \$188 per record*

“doblarse pero no romperse”

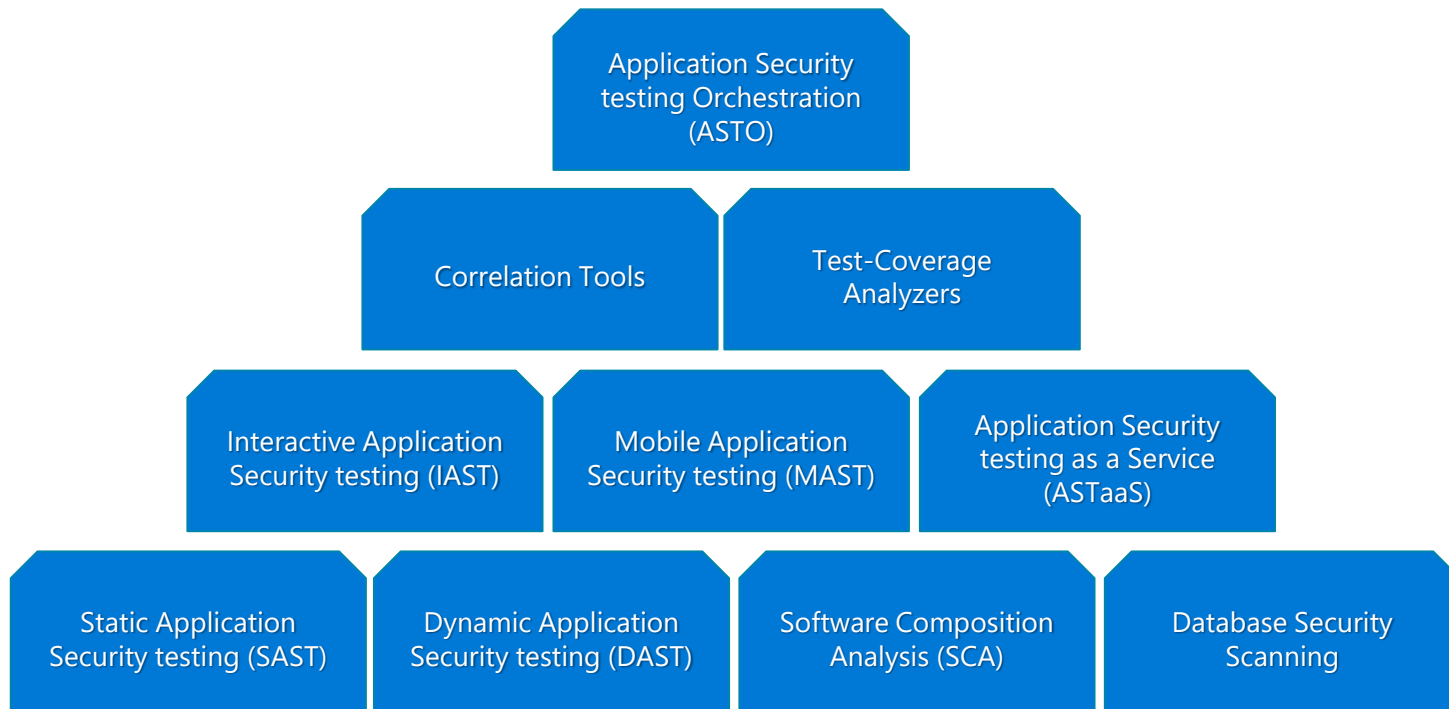
**La forma de mitigar la
incapacidad de anticipar los
ataques de las nuevas
vulnerabilidades de día cero**



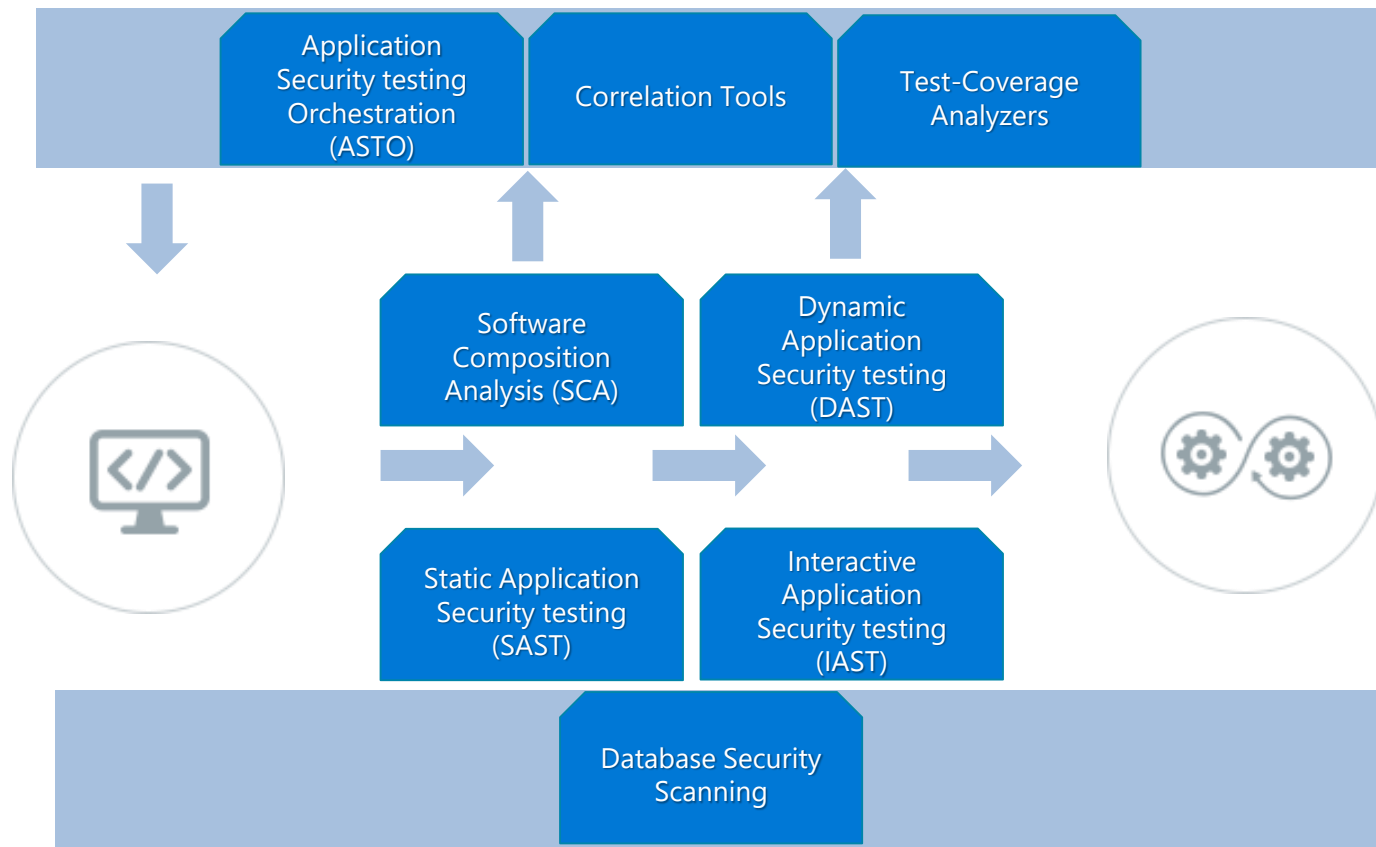
DevSecOps | Técnicas y practicas



AST (Application Security testing tools)



Application Security Testing Tools Reference Model CI/CD Development Project



DevSecOps - Argentina



<https://www.linkedin.com/groups/12033278/>



<https://marketplace.visualstudio.com/azuredevops>







Azure DevOps + AST (Application Security testing tools)



30 Results



Showing: Azure Pipelines ▾ Hosted On: Any ▾ Price: Any ▾ Sort By: Relevance ▾



**Container Security**
Aqua Security  315
Vulnerability scanner for container images
★★★★★ FREE



**Secure Secrets**
Kevin Hagmaars  44
Create or generate Azure Key Vault secrets and put them directly in your Azure Key...
★★★★★ FREE



**Serverless Security**
Aqua Security  38
Vulnerability scanner for serverless
★★★★★ FREE



**Secure Files**
Carlo Wohlfeldt  269
Allows you to download the secure files stored in the library
★★★★★ FREE



**Secure Zip**
Delta N BV  84
Archive / Extract files or folders protected with a password
★★★★★ FREE



**Secure DevOps Kit (A)**
Microsoft DevLab  1,28
Collection of extensions that empower DevOps teams to build and deploy applications...
★★★★★ FREE



**Micro Focus Fortify**
Fortify  3,33K
Use the Micro Focus Fortify VSTS build tasks in your continuous integration build...
★★★★★ FREE



**SD Elements Integrati**
Security Compass  4
Security Compass SD Elements Platform Integration
★★★★★ FREE



**Black Duck Detect**
Synopsys  334
Run Black Duck Detect for your build
★★★★★ FREE



**Puma Scan Professional**
Puma Security  12
Puma Scan is a software security source code analysis extension that scans code fo...
★★★★★ PAID



**Codified Security**
Codified Security  55
This step uploads your app to Codified Security for automated mobile app...
★★★★★ FREE



**Application Security**
HCL Technologies  39
Perform static, dynamic, mobile and open source security tests for your...
★★★★★ FREE



**Download Secure File**
Matt Labrum  476
Downloads a secure file
★★★★★ FREE



**API Management Suite**
Stephane Eykens  628
Broad support of Azure API Management
★★★★★ FREE



**Kluwan**
Kluwan Software  123
Analyze your applications with Kluwan in your build definitions. Find relevant...
★★★★★ FREE



**Checkmarx CxSAST**
Checkmarx  1,7K
Add Secure Static Source Code Analysis inside your build process
★★★★★ FREE



**Install SSL and Custom Triple**
Triple  69
Adds a .PFX secure file and custom domains to an App Service in Azure
★★★★★ FREE



**WhiteSource**
WhiteSource  1,2K
Detect & fix security vulnerabilities, problematic open source licenses and...
★★★★★ FREE



**FOSSA**
Fossa  32
Automatically analyze your code for open source license compliance and security...
★★★★★ FREE



**WhiteSource Bolt**
WhiteSource  2,5K
Detect & fix security vulnerabilities, problematic open source licenses.
★★★★★ FREE



**Snyk Task**
Jesse Houwing  198
Snyk continuously finds and fixes vulnerabilities in your dependencies.
★★★★★ FREE



**OWASP Zed Attack Proxy**
Kasun Kodagoda  770
Visual Studio Team Services build/release task for running OWASP ZAP automated...
★★★★★ FREE



**Code Dx - Run Analysis**
Code Dx  24
Upload files to your Code Dx server to run an analysis
★★★★★ FREE



**IP Address Scanner**
Swiftlab  45
A build/release task for scanning the IP Addresses from the activity of your...
★★★★★ FREE



**SSL Labs Test**
Kasun Kodagoda  90
Analyse the SSL configuration of any public web server using the Qualys SSL Labs S...
★★★★★ FREE

**Dotfuscator Community**
PreEmptive Solutions  598
Protect the value of your software innovation and the integrity of your .NET...
★★★★★ FREE

**Veracode**
Veracode  2,6K
Find and fix security defects as part of your Azure DevOps pipeline - v2.4.0
★★★★★ FREE

**FlexNet Code Insight**
Flexera  29
Run a Code Insight scan as part of your build
★★★★★ FREE

**MyGet Package Manager**
MyGet  1,5K
Securely create, host, manage, and share NuGet, symbols, rpm, Docker, Maven, PIP...
★★★★★ FREE

**AppVeyor CI**
Appveyor Systems  187
Continuous Integration service for Windows developers that securely...
★★★★★ FREE

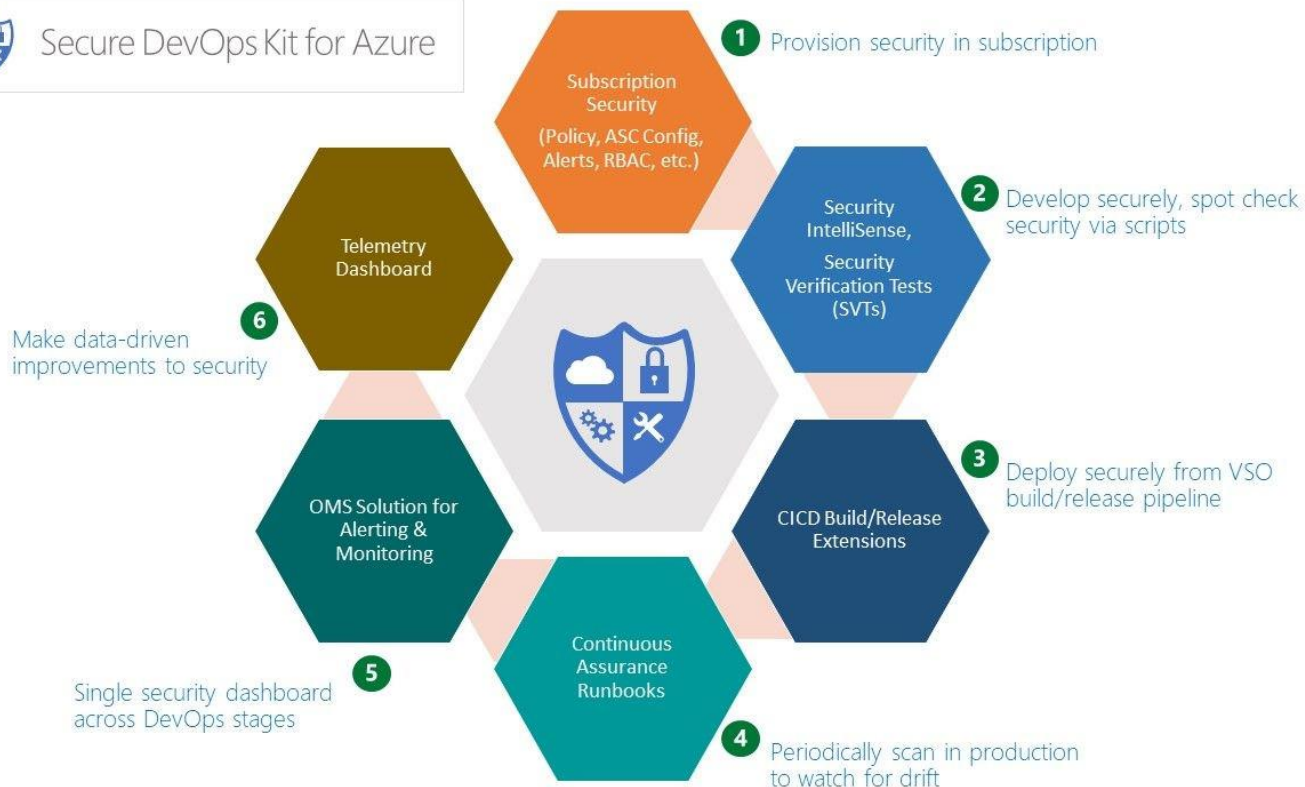
DEMO: Azure + AST

¿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)
- 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



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:

I. 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.

Las herramientas principales incluyen:

- **Health Check Script:** para problemas de seguridad, configuraciones erróneas o configuraciones obsoletas
- **Script de provisión:** para control de acceso, alertas, políticas, contactos, Políticas de Azure Resource, Configuración de la política empresarial predeterminada para Azure Security Center

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.

Las herramientas principales incluyen:

- **Pruebas de verificación de seguridad (SVT):** controles de seguridad incorporados para los servicios de Azure. 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:** guía sobre las mejores prácticas de codificación segura. 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



Los componentes de . **Security in CI/CD** ayudan con 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.

Las herramientas principales incluyen:

- **Extensión de AzSDK para VSTS:** es privada, se debe solicitar para
✓ Tarea de Build /Release para pruebas de verificación de seguridad
- **(SVTs):** en el pipeline de CI / CD

4. Continuous Assurance



La **Continuous Assurance** evita la desviación 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.

Las herramientas incluyen:

- **Runbooks de Azure Automation:** que identifican y corrigen los desvíos de la configuración de seguridad.
- **Plantillas de Azure Resource Manager:** que se utilizan para implementar de manera segura los recursos de Azure preconfigurados.
- **Scripts de PowerShell:** es 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.

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.
- 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. Se enruta a una cuenta de Application Insights, 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.

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.** 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 usuario

DEMO: Secure DevOps Kit for Azure

¿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 DevSecOps

4

Procesos sencillos para comprobar las soluciones existentes

5

Comprobaciones de seguridad más sencillas y resolución de problemas

6

Siguiendo metodologías de desarrollo ágil

7

Buscando automatizar sus procesos de desarrollo

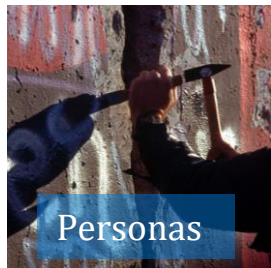
8

Creación de aplicaciones de alta seguridad para los principales clientes

9

Con el objetivo de reducir los costos para garantizar la seguridad

Conclusiones



Colaboración
Fin de las divisiones
Acercamiento entre áreas
Cambio de comportamiento



Acompañar las investigaciones, nuevas metodologías, herramientas etc.... estar en la cresta de la ola



Hagamos todas las revisiones de seguridad lo mas temprano posible en el proceso de desarrollo. Prod es tarde



"todo"
Desplegar
Control
Monitoreo
SCM
Orquestación



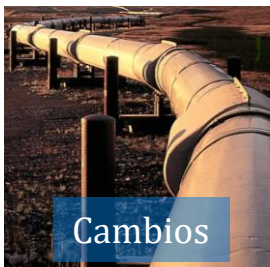
¡ Siempre asumamos la existencia de la brecha!



Todo es trazable: Debemos ser capaces de rastrear un cambio en su origen: Quién solicitó el cambio, creó el cambio, aprobó el cambio etc...



¿Es necesario explicar?



No hay cambios en la producción sin un pipeline controlado



Microsoft

Thank You

ευχαριστώ Salamat Po متشكراً شكراً Grazie
благодаря ありがとうございます Kiitos Teşekkürler 谢谢
ឧបត្ថម្ភ Obrigado شكریه Terima Kasih Dziękuję
Hvala Köszönöm Tak Dank u wel ДЯКУЮ Tack
Mulțumesc спасибо Danke Cám ơn Gracias
多謝晒 Ďakujem תודה நன்றி Děkuji 감사합니다