AVALORA

Boosting
human
capabilities

¡Comenzamos en unos minutos!

Cybersecurity
Rpa consulting
Infrastructures & Cloud
Digital Solutions

avalora.com

Madrid
Stgo
Lima

VERACODE

‘El Conflicto Eterno: Seguridad vs Desarrollo’

2020

Joost de Jong
Director LATAM & Caribe

Special Presentation: AVALORA

Sobre Veracode

AVALORA

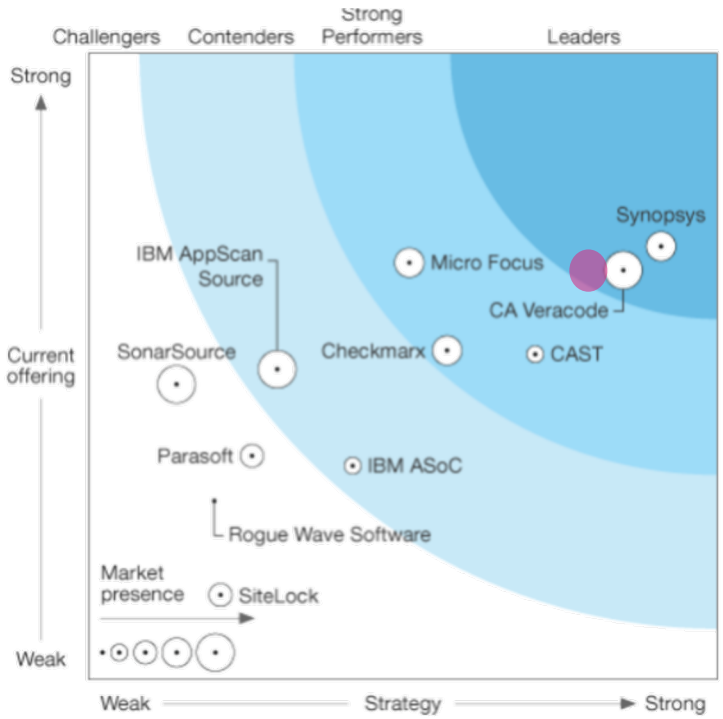
Gartner Magic Quadrant for Application Security Testing 2020

Magic Quadrant

Figure 1. Magic Quadrant for Application Security Testing

Source: Gartner (April 2020)

Forrester Wave™: Static Application Security Testing Q4 2017

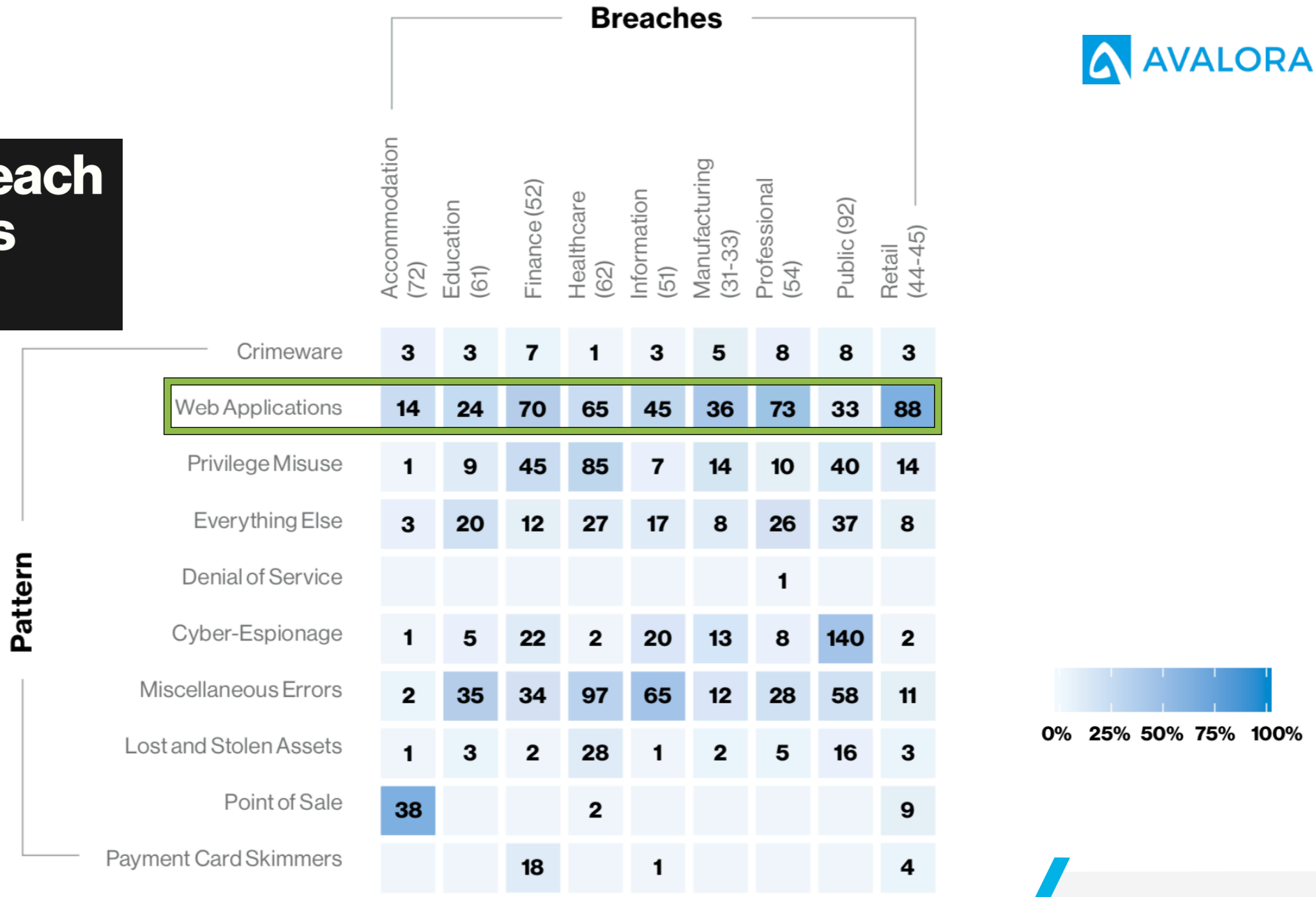


- Sede principal, Boston, USA
- Fundado en 2006
- Empresa 750 empleados, 350 ingenieros
- Dedicado a: Application Security Testing
- SAST / DAST / SCA / IAST
- Lider Mundial

verizon business ready

2019 Data Breach Investigations Report

AVALORA



AVALORA

DevSecOps
Version LATAM

En América Latina, casi
350 millones de personas tienen acceso a Internet mediante sus teléfonos inteligentes.

El consumidor digital exige nuevos modelos de negocios y, el sector financiero se está transformando con rapidez.

100 millones
solamente en Brasil

Como Cambia la Entidad en Contestacion a la Transformacion Digital?

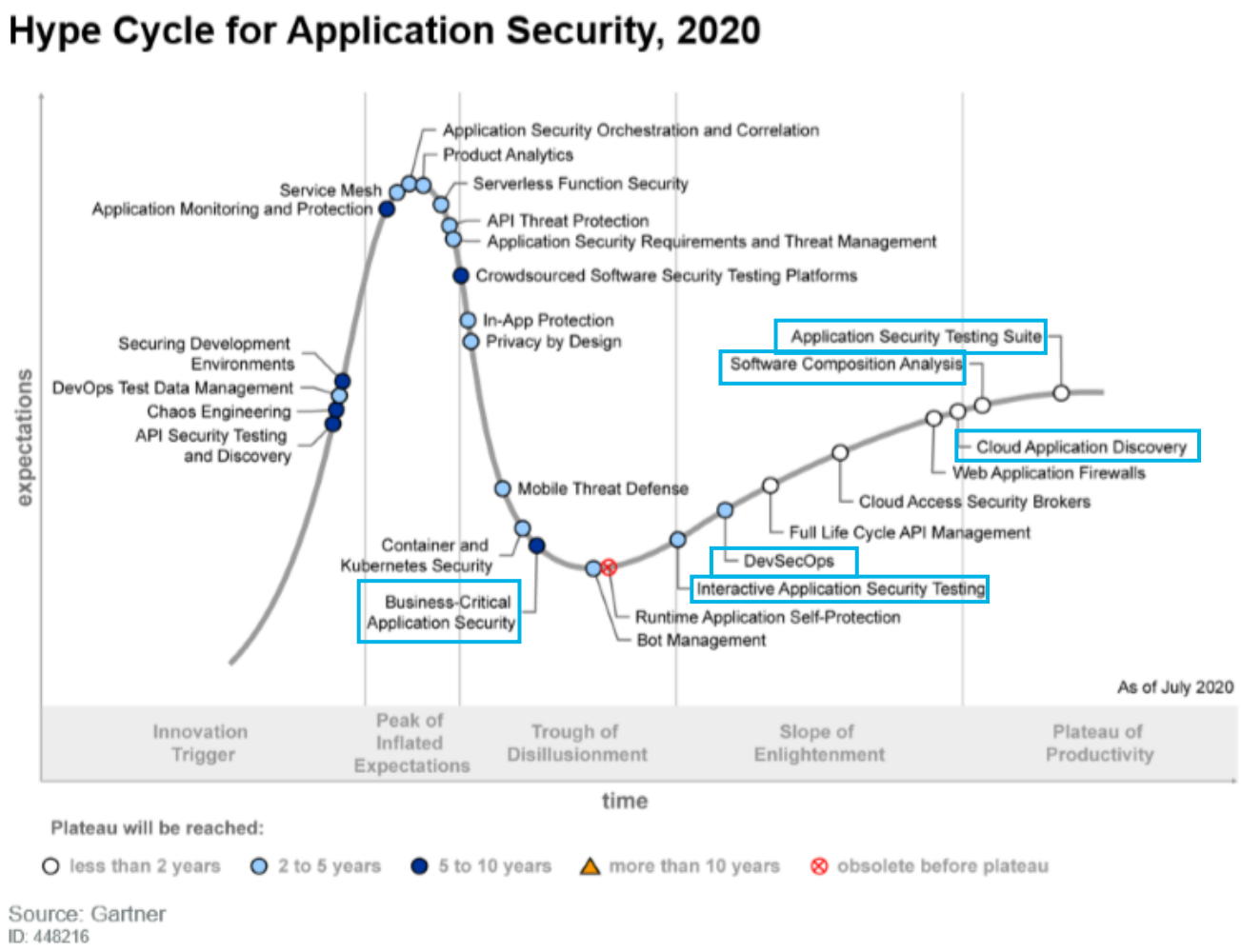
- Comunicamos con los Clientes a traves de Apps y Aplicaciones.
- Presion Aumentar la Capacidad de Desarrollar Codigo (Interno y Fabricas)
- Presion de Versionar Mas Rapido

Consideraciones: *DevSecOps*

AVALORA

- Time-to-Market / Eliminar Atascos en el SDLC: *Las empresas mas ágil en Desarrollo pueden dominar el mercado*
- Compliance: *Las leyes adaptan a la realidad*
- Seguridad Verdadera – *La mitigación de las vulnerabilidades encontradas es dirigida por la frecuencia de la interacción entre Desarrollo y Seguridad*
- Políticas Centralizadas: *No es practica tener políticas por cada app o depender sobre decisiones de individuales*
- Escalar a todos los Apps: Desarrollo propio y Fabricas de Software. *(Aunque una App no es prioridad para ti, esto no implica de que no tiene acceso privilegiado a tus sistemas)*

Technology Curve



Source: Gartner
ID: 448216

Tendencias

- En vez de ‘point solutions’ encontramos mas demanda para ‘solutions suites’ cuales cubren el SDLC entero.
- Enfoque hacia la revisión del código ‘en proceso’ en vez de al final del ciclo
- El SCA ya forma parte imprescindible del proceso Application Security Testing.

AVALORA

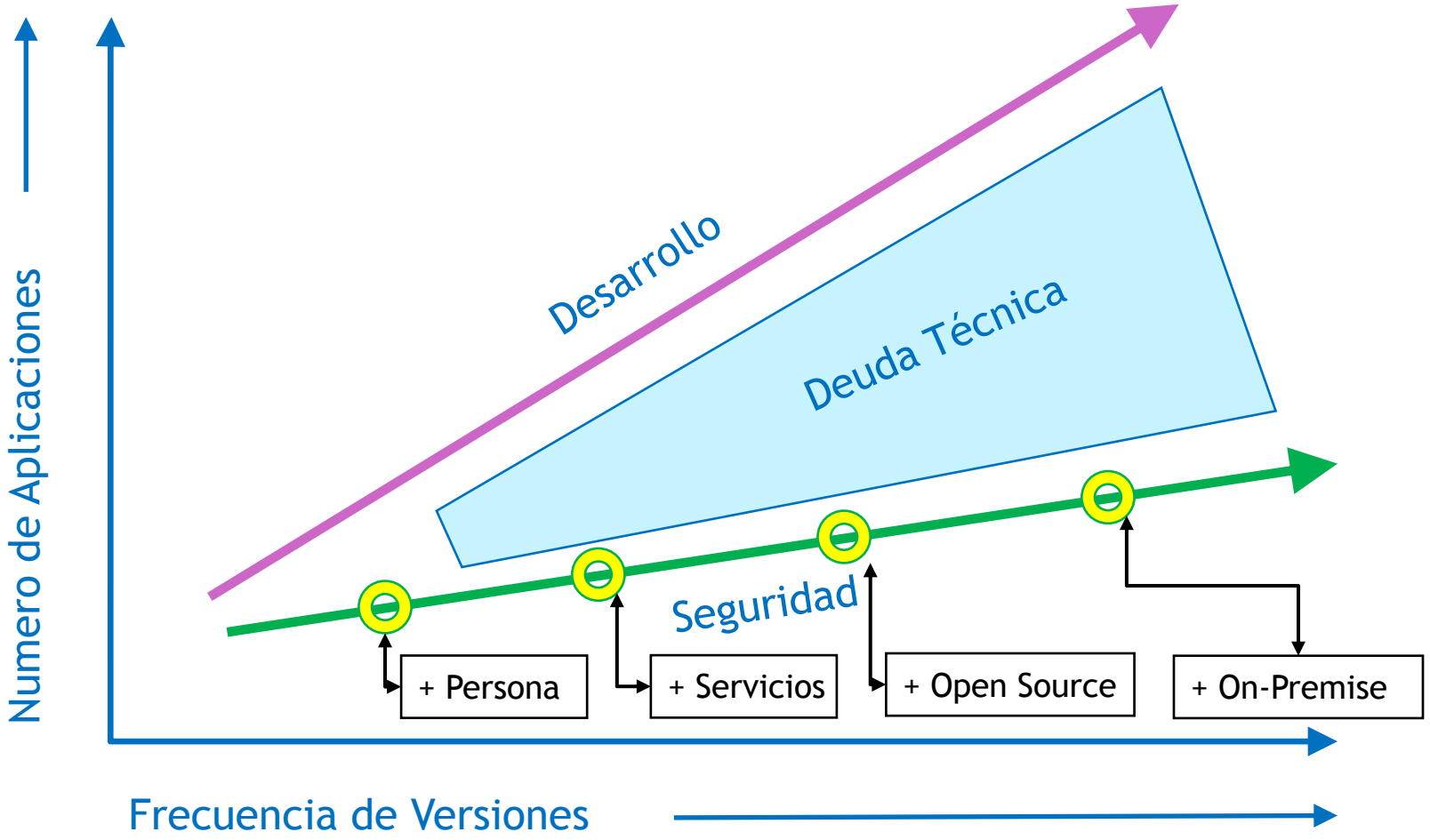
Desarrollo: Entre los Business Units & Seguridad

VERACODE

Desarrollo y Seguridad a la Misma Velocidad

AVALORA

Velocidad o Seguridad?

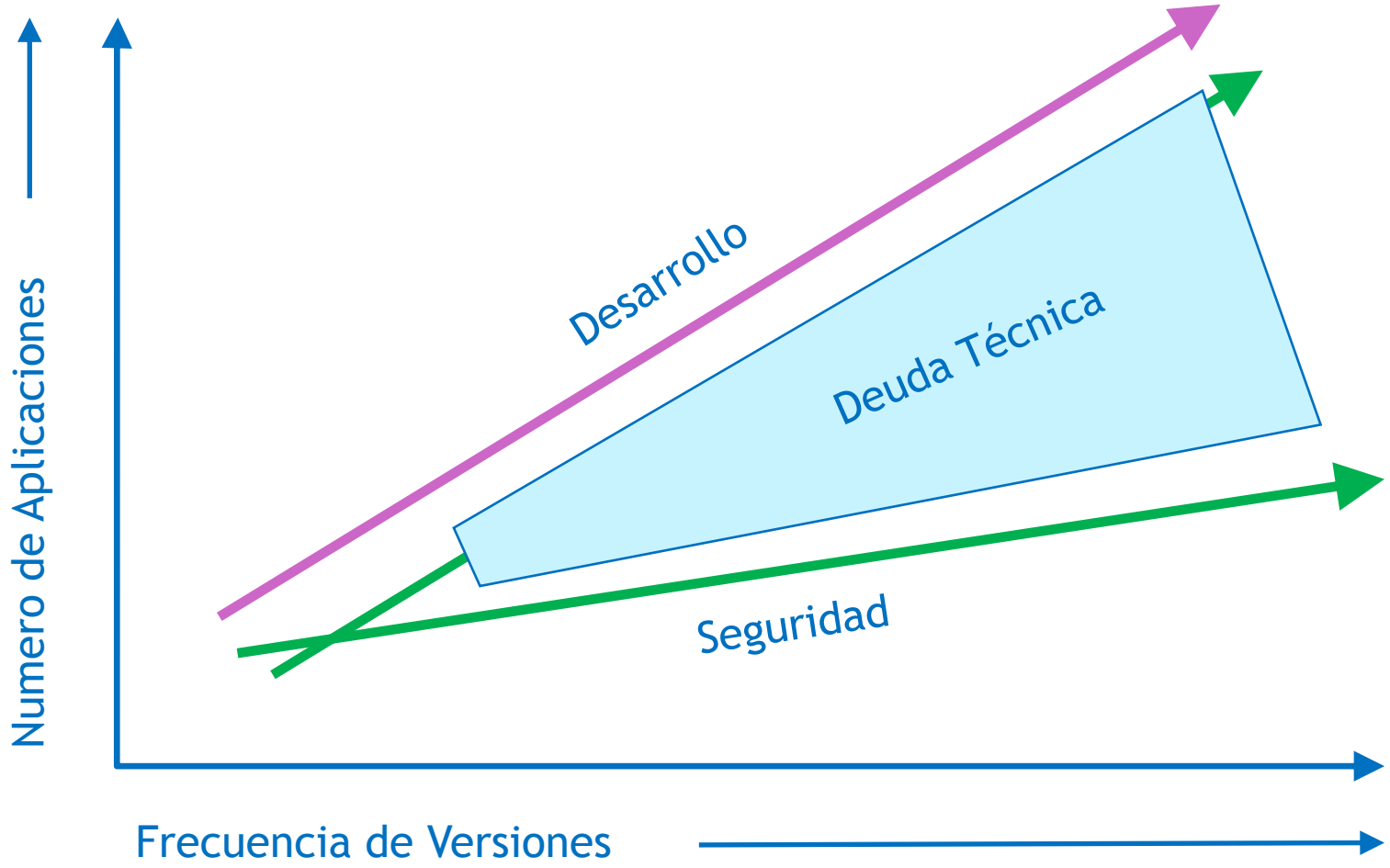


VERACODE

Desarrollo y Seguridad a la Misma Velocidad

AVALORA

Velocidad o Seguridad?



VERACODE

Compliance
Version 2020

AVALORA

Colombia: Circular 7 & 8

Estándares Nuevas por la sector financiera en Colombia. Exige no solo cumplir con normativas pero también certificar y documentar procesos, tanto dentro la entidad mismo pero también aplica a los procesos de proveedores. Capitulo: 3.8 y 3.9

USA: PCI S3

Enero 2019, las normativas yo no piden revisión una vez pero procesos y practicas documentados, la inclusión de módulos Open Source: Secure SLC Requirements (SSLC);

EU: GDPR

Exige Procesos Documentados, Seguridad en el Ciclo de Desarrollo, y prestan la responsabilidad a la entidad de ser capaz de responder con informacion detallada en caso de incidencia. // Requiere que una persona lleva la responsabilidad // Controller – Responder en 72 horas

Brasil: LGPD

LGPD es normativa vigente en Brasil cual encuentra su base en el GDPR. Igual exige procesos documentadas y buenas practicas en el SDLC entera.

Estandares: Con requerimientos AppSec

- Seguir Flaws y Errores
- Identificación y Mitigación de Vulnerabilidades en el SDLC
- Automatización

Nueva Normativa, El Salvador

Adquisición, desarrollo y mantenimiento de sistemas informáticos

Art. 21.- Para la administración de la seguridad en la adquisición, desarrollo y mantenimiento de sistemas informáticos, las entidades en lo aplicable, deben tomar en cuenta como mínimo lo siguiente:

a) Incluir controles al ingreso, acceso, transmisión, procesamiento y salida de información;
b) Aplicar las técnicas de cifrado que garanticen efectivamente la protección del almacenamiento y transporte de la información crítica de acuerdo a la clasificación de la entidad;
c) Definir controles sobre la implementación de aplicaciones antes del ingreso a producción;
d) Controlar el acceso al código fuente de los sistemas informáticos que son propiedad de la entidad;
e) Mantener un estricto y formal control de cambios y versiones, que será debidamente apoyado por sistemas informáticos en el caso de ambientes complejos o con alto número de cambios;

f) Contar con mecanismos de desarrollo seguro que permita analizar y corregir las vulnerabilidades de seguridad existentes en las aplicaciones informáticas de la entidad. Deberá efectuarse este tipo de análisis en el ciclo de vida del desarrollo de dichas aplicaciones y establecer los procedimientos de corrección adecuados; asimismo, cuando dichos sistemas se encuentren en producción; y
g) Establecer un procedimiento de instalación de actualización de software, de forma segura y controlada, con el objeto de prevenir vulnerabilidades y sin afectar el desempeño de la infraestructura.

Compliance con Veracode

STANDARD	SECTIONS/CONTROLS SUPPORTED
PCI-DSS	6.1, 6.5, 6.6, 6.7, 11.3, 12.6
PA-DSS	5.1.7, 5.2, 7.1
HIPAA/HITRUST CSF	01.v, 02.e, 04.a, 06.d, 10.a, 10.b, 10.c, 10.l, 10.m
NIST 800-37	Tasks 1, 4, 5, 8, 9, 10
NIST 800-53	AT-2, 3, 4; CA-2, 7, 8; CM-4, 8; RA-2, 3, 5; SA-3, 4, 11, 12; SC-13; SI-2, 7, 10, 11, 12; PM-1, 6, 14
NIST 800-161	Controls for 800-53, plus AU-10; CM-7, 8; CP-2; PV-1, 2; RA-1; SA-8, 11, 12
New York Department of Financial Services Cybersecurity Regulations	500.05(a) 1,2; 500.06(a)2; 500.08(a); 500.11; 500.14(a)2
Monetary Authority of Singapore Technology Risk Management Guidelines	5, 6, 9.4, 12.2
Sarbanes-Oxley	Fraud prevention; protection of audit trails
OCC Bulletin 2013-29	Requires regulated entities to assess and manage risks associated with their third-party relationships
Securities and Exchange Commission Requirements for Cybersecurity	SEC has published guidance for public companies related to the disclosure of cybersecurity risks and the financial impact of cyber incidents such as data breaches. We can help by providing detailed analytics about the current risk profile for your application infrastructure as well as an assessment of the remediation work required after a successful application-layer attack.
FS-ISAC Third Party Software Controls	Control Type 2, 3a, 3b
GDPR	Articles 5, 22, 23, 26, 30, 31, 33

Actualización:

Circular 7 & 8 (Colombia)

GLPD (Brasil)

AVALORA

VERACODE

Compliance: Circular 7 & PCI S3

Versión 2020

AVALORA

Circular 7, Capítulos 3.8 y 3.9 (Cubre el SDLC y Software de Terceros)

3.8. Incluir dentro del ciclo de vida del desarrollo del software, incluyendo servicios web y *apps*, que procesan la información confidencial de la entidad o de los consumidores financieros (desde las etapas iniciales tales como levantamiento de requerimientos hasta las pruebas de seguridad pertinentes y producción), aspectos relativos con la seguridad de la información que permitan mitigar dicho riesgo.

3.9. Incluir en los contratos que se celebren con terceros críticos, las medidas y obligaciones pertinentes para la adopción y el cumplimiento de políticas para la gestión de los riesgos de seguridad de la información y ciberseguridad.

PCI S3 Secure Software Lifecycle (Secure SDLC Standard)

"Address common coding vulnerabilities in software-development processes as follows:

- Train developers at least annually in up-to-date secure coding techniques, including how to avoid common coding vulnerabilities.
- Develop applications based on secure coding guidelines."

"Verify that processes are in place to protect applications from, at a minimum, the following vulnerabilities: Injection flaws, Buffer overflows, Insecure cryptographic storage, Insecure communications, Improper error handling, XSS, Improper access control, CSRF and Broken authentication and session management."

VERACODE

Frecuencia de Escaneo

y tiempos de remediación

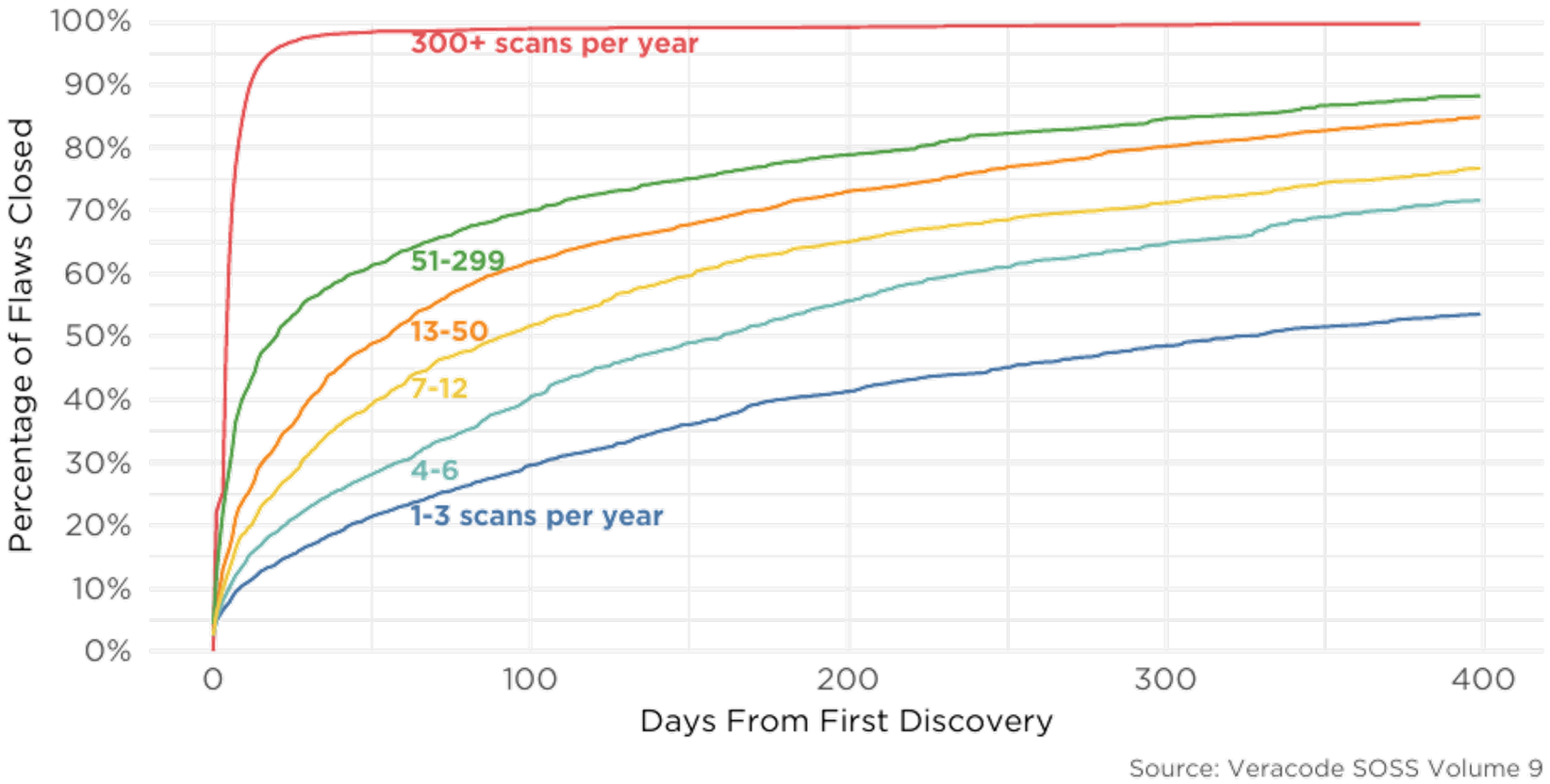
AVALORA

Mitigación:

Las entidades que revisan su aplicaciones con alta frecuencia (300+ al ano) llegan a '0' vulnerabilidades fuera de su políticas – *obviamente sin automatización y la inclusión a todos involucrados en el SDLC desde el principio seria imposible lograr estas metas*

NOTA: Los que revisan sus aplicaciones entre 1-3 veces al ano dejaran el 50% de las vulnerabilidades identificados en el código publicado

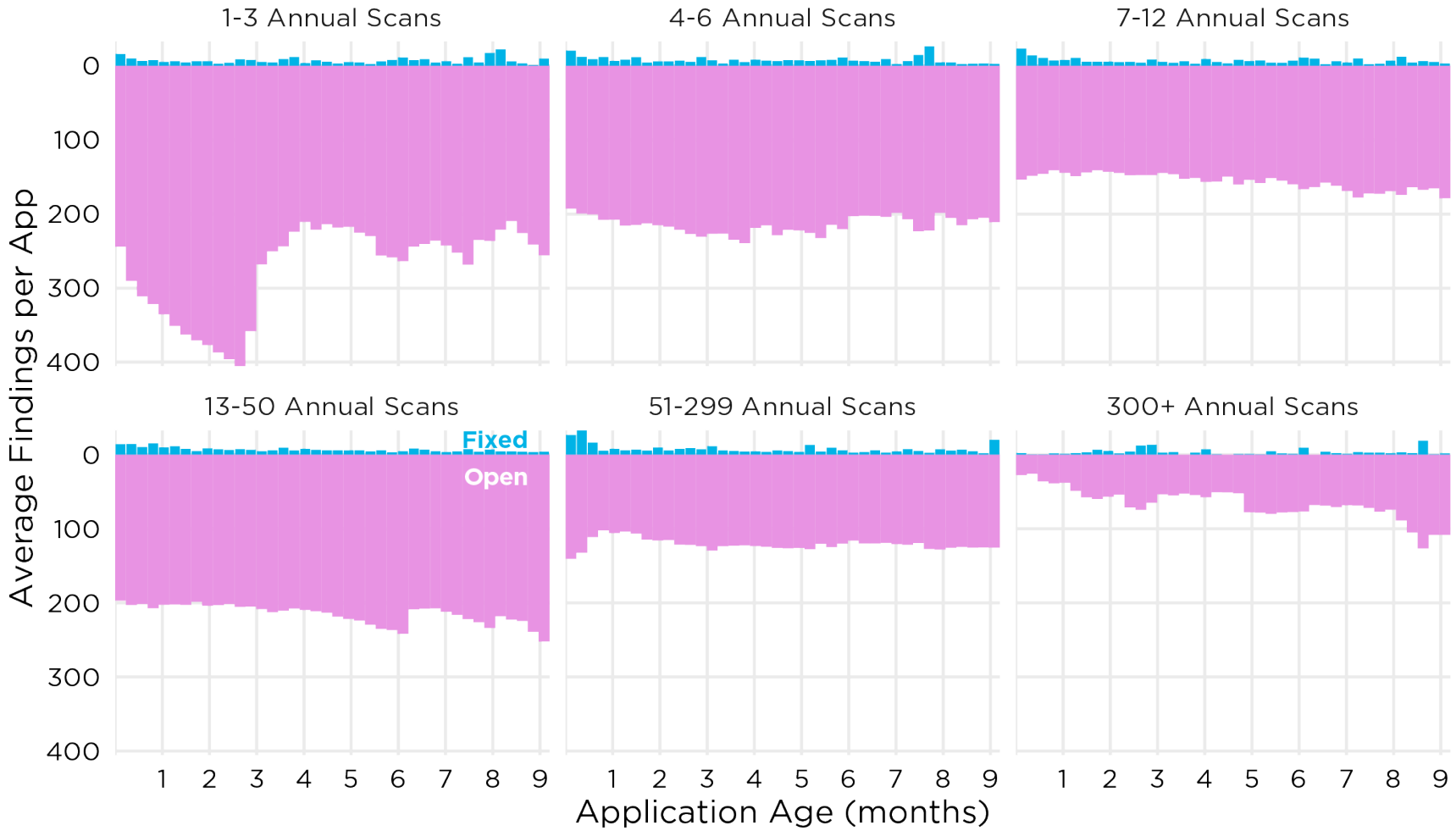
Clientes Veracode resuelven unos 70% de las vulnerabilidades identificadas, una mejora de 12%



Source: Veracode State of Software Security, Vol 9

Impacto del proceso ‘DevSecOps’

AVALORA



Source: Veracode SOSS Volume 10

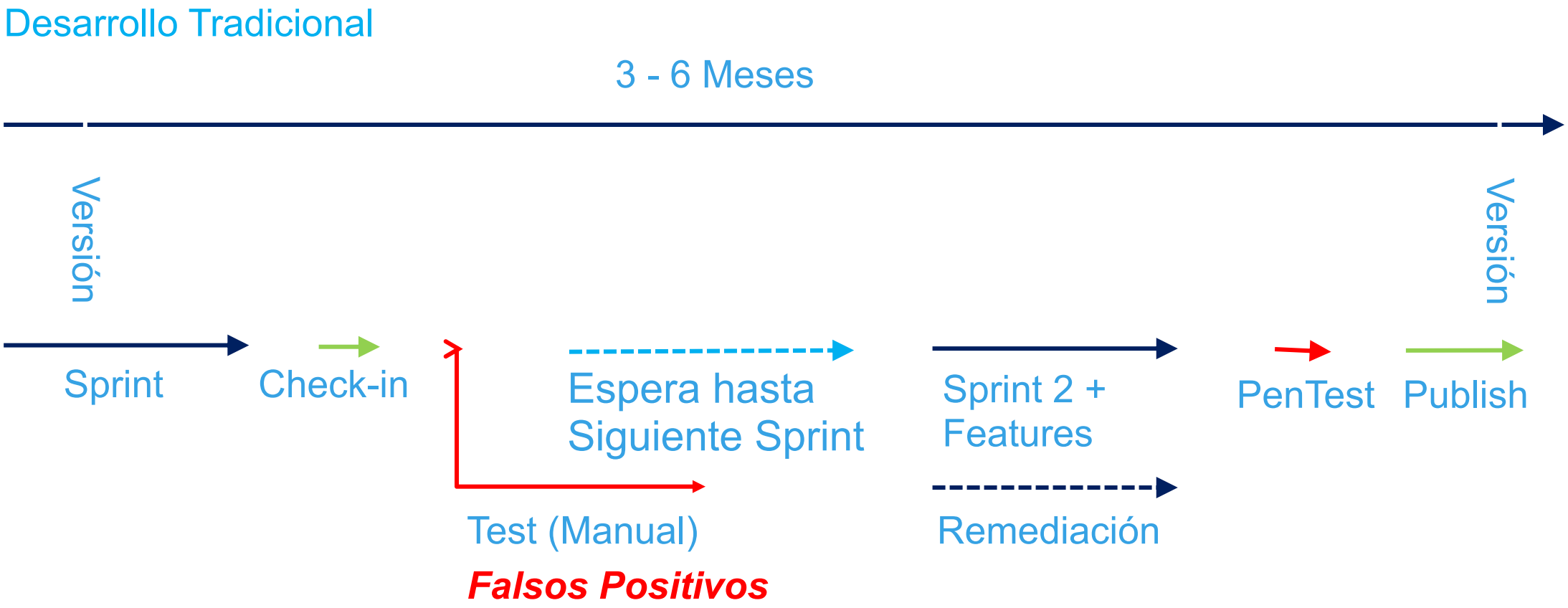
5X

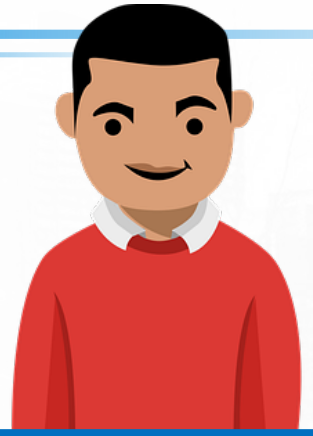
Reduccion en Deuda Tecnica

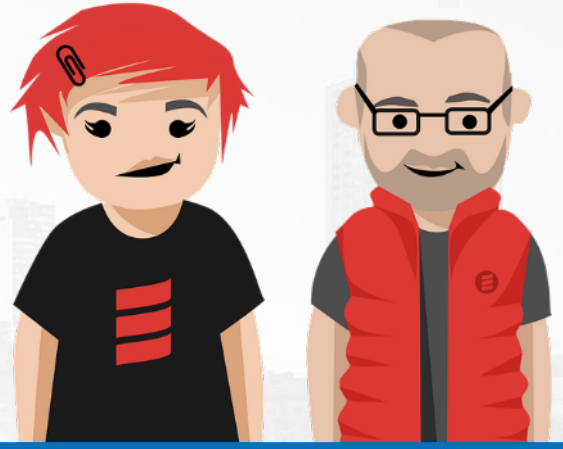
VERACODE

Procesos de Verificacion de Seguridad Manual:

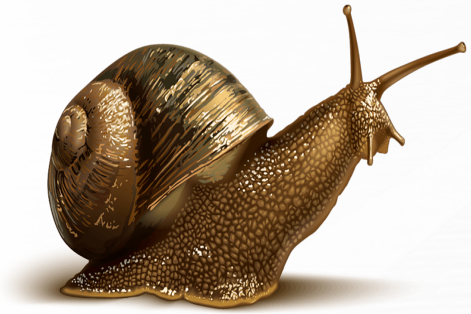
Atasco Principal en el SDLC







Velocidad de Entrega

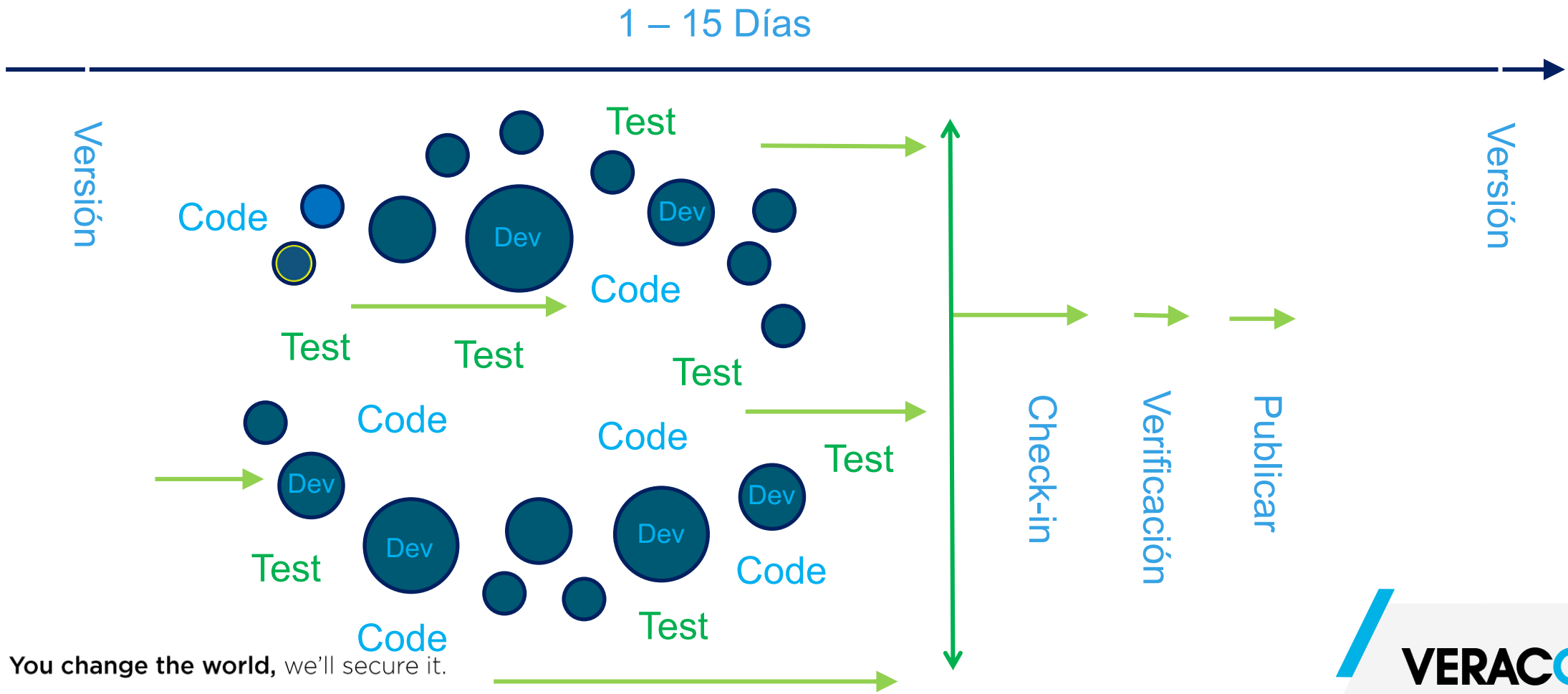


AVALORA

AVALORA

DevSecOps

Desarrollo DevSecOps – Eliminando la Separación entre Dev y QA/Seguridad

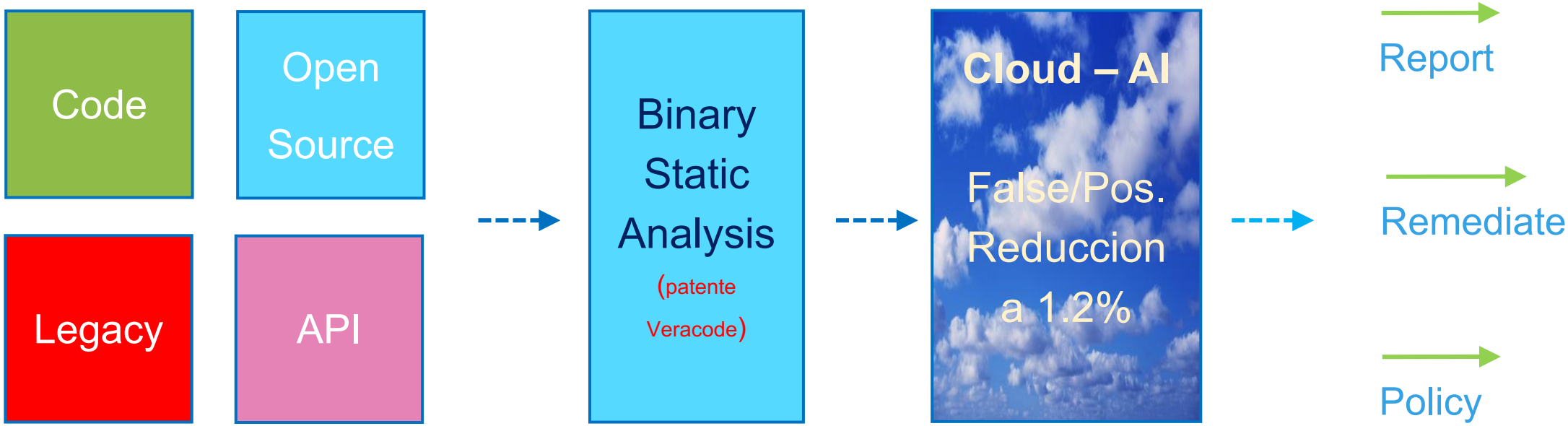


VERACODE

Veracode

AVALORA

Liberar el Desarollador de ser Experto en Seguridad



Forman la ‘Aplicación’

Politicas y Resultados Uniformes

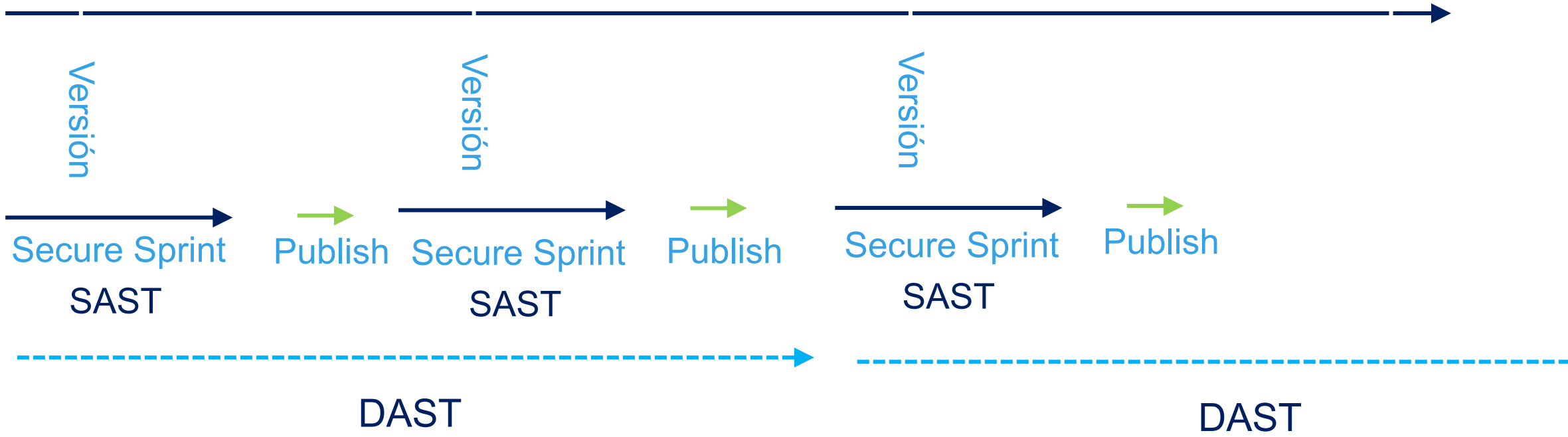
You change the world, we’ll secure it.

VERACODE

Procesos DevSecOps:

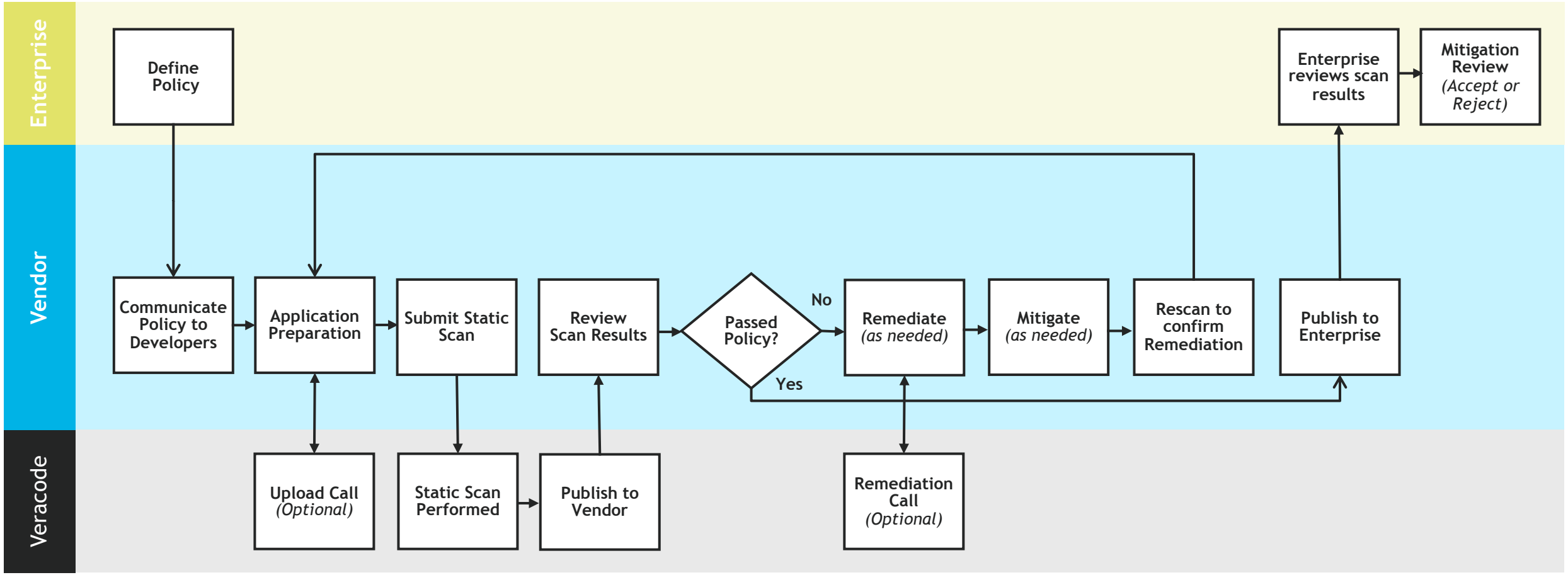
Desarrollo Rapido y Seguro

Sprints: *Solo los cambios necesarios*



Fabricas de Software – Politicas AppSec

Eliminar el Ciclo ‘Hacer’, ‘Entregar’, ‘Test’, y ‘Rehacer’



AVALORA

VERACODE

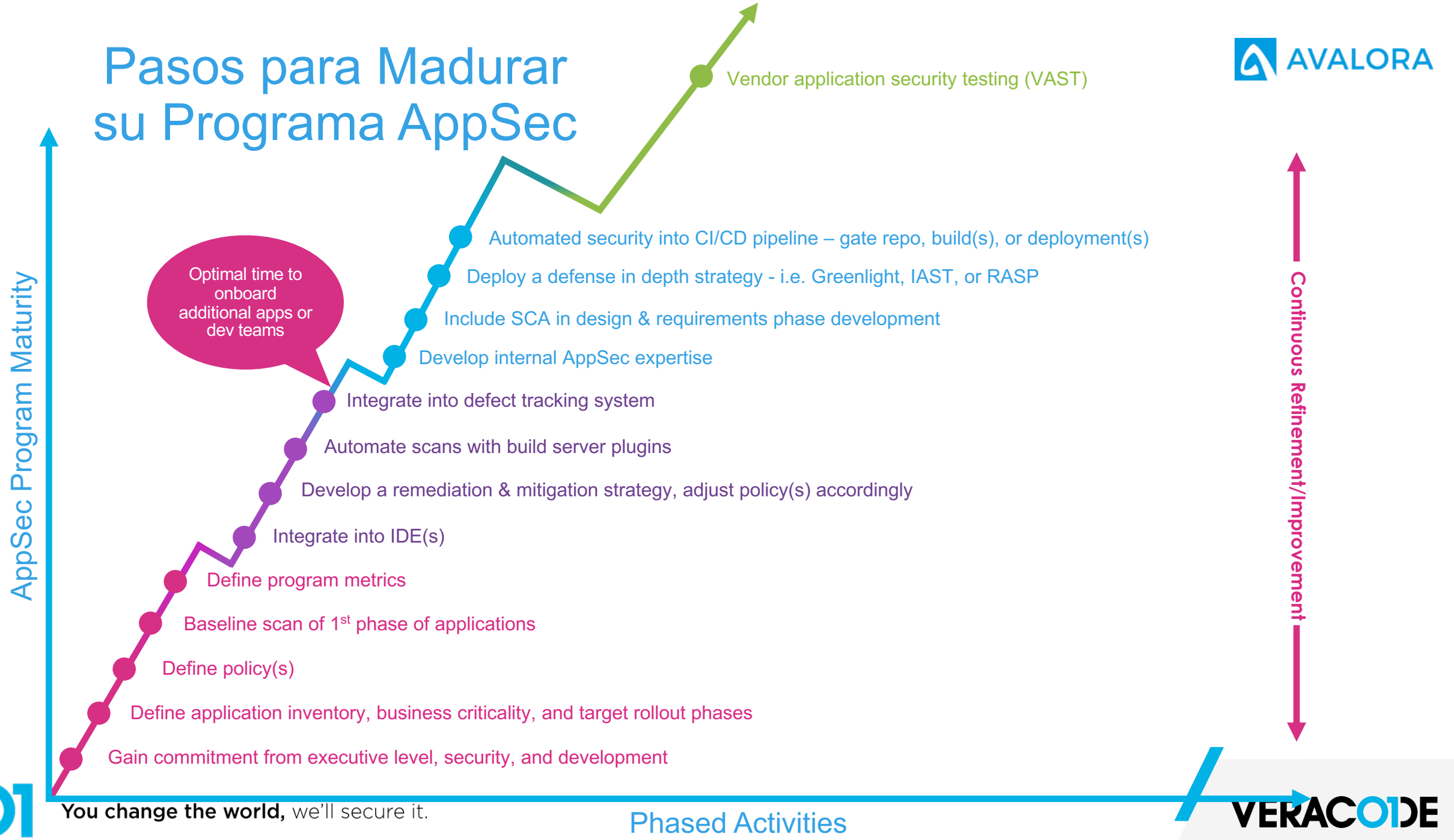
Destinos del ‘Viaje hacia el DevSecOps’

AVALORA

- Políticas Centralizadas y Uniformes por la entidad: Seguridad Verdadera
- Aceleración del SDLC y Time-to-Market (La clave para mantener posición competitiva) Objetivo: -90% por Versión
- Cumplir con las nuevas normativas como PCI 2019 / Circular 7 (Colombia), OWASP, SANS y CERT que exigen procesos documentados y buenas practicas
- Reducción de Costes: 90+% por Versión de Software

VERACODE

Pasos para Madurar su Programa AppSec



AVALORA

VERACODE

You change the world, we'll secure it.

VERACODE

Gracias

2020

AVALORA