



0xFF SDLC

Abril 2017





Agenda

- + Quienes somos?
- + SDLC
- + Contexto
- + Threat model
- + Code review
- + Open Source Security
- + Issue Tracker
- + Wiki
- + Metricas

Hola!

- Alejandro Iacobelli
- Alexander Campos

Contactanos:

- alejandroiacobelli@mercadolibre.com
- alexander.campos@mercadolibre.com





Our job

- + SecDevOps (Automatizaciones y desarrollos)
- + Consultoría de seguridad
- + Cursos de seguridad
- + Pentest, Code Review, BugBounty Interno, reportes de onda
- + Manejo de vulnerabilidades
- + Administración de WAF
- + Bug Bounty players
- + Monitoreo de seguridad



SDLC

El ciclo de vida de desarrollo (SDL) es un proceso que ayuda a los desarrolladores a construir software más seguro, reduciendo costos y tareas.

Contexto - Tipos de empresa

Producto sin Seguridad

Seguridad despues del
Producto

Seguridad antes que el
Producto

Con que nos encontramos

Seguridad
despues del
Producto

No tengo tiempo!
Objetivos vs. Seguridad



Keep it simple

Unidades de negocio
descentralizadas



Detect detect detect

1 persona de seguridad cada
300 developers



Automatizar y autogestionar

Soluciones comerciales poco
customizables y caras



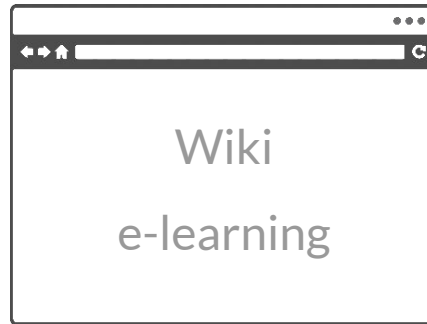
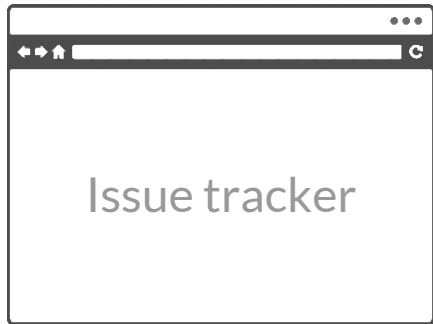
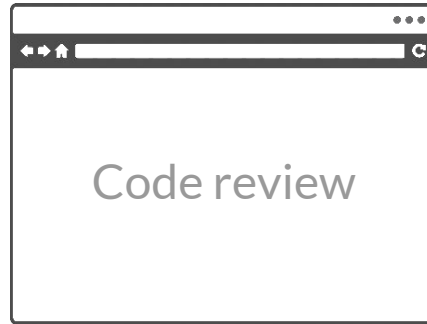
Customizable

Recambio constante de
desarrolladores y tecnologías



Transmisión de conocimiento escalable
Modularizada

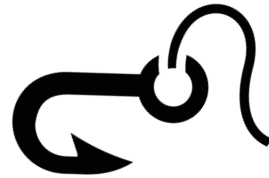
Fantastic framework for SDLC





Threat Model Automatizado

Detección de nuevos proyectos - Fase 1



+ 5 security questions

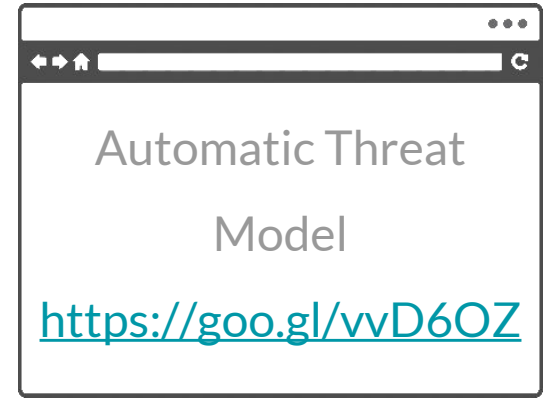


Detección de nuevos proyectos - Fase 2

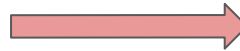
+ 5 security questions



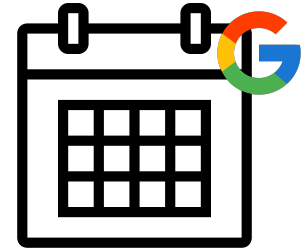
low / medium



high



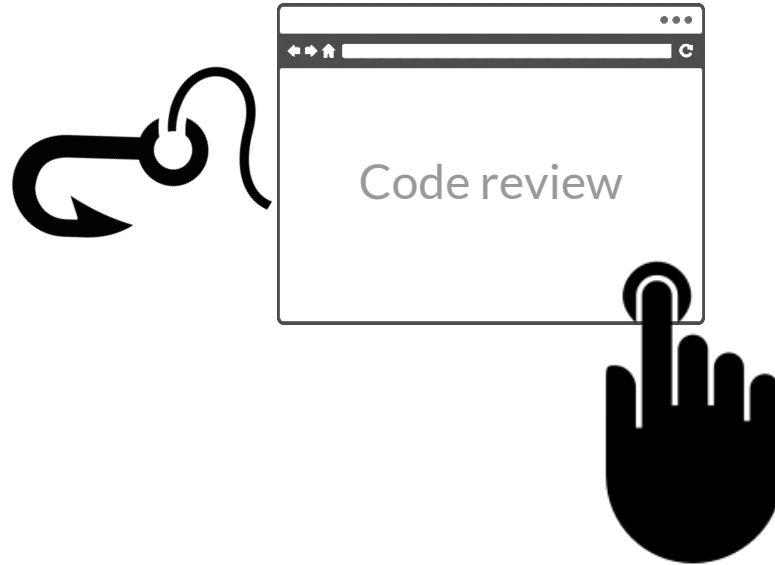
/GET





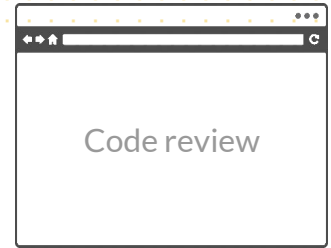
Code Review Automatizado

Modificación de proyectos existentes



Code review - AFIP

- + Análisis de código estático
- Manejo de falso positivo
- Rule based approach
- Mantenable en el tiempo
- Adaptable a la empresa





Open Source Security

Análisis de librerías

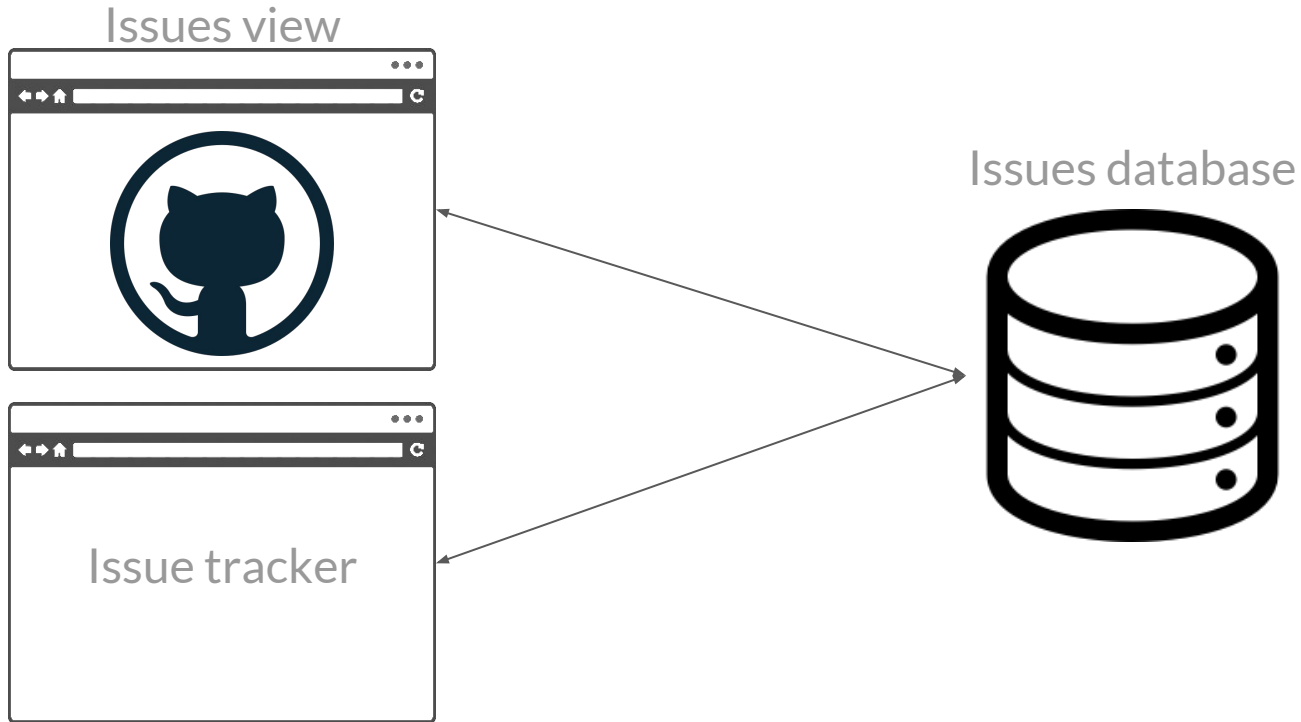


- + Armado de inventario de librerías del proyecto a analizar
- + Asociar vulnerabilidades conocidas publicadas en sitios confiables y relacionarlas (OWASP Dependency Check, nsp)
- + Informar de aquellas con vulnerabilidades

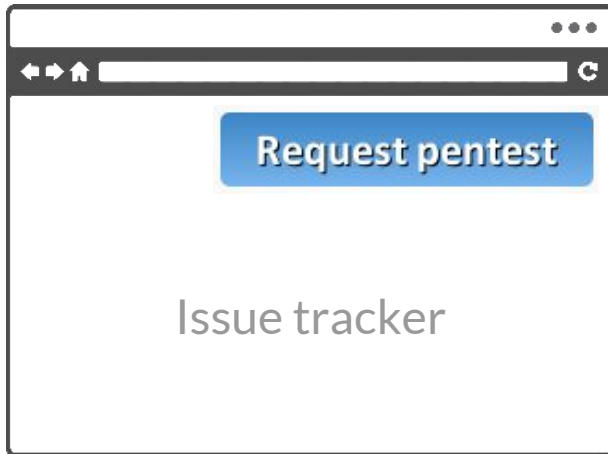
The background of the slide is a photograph of a forest with many tall, thin trees. The entire image is covered with a semi-transparent yellow filter and a white dot grid pattern. The text is centered in the middle of the image.

Issue tracker Automatizado

Issue Tracker



Pentest

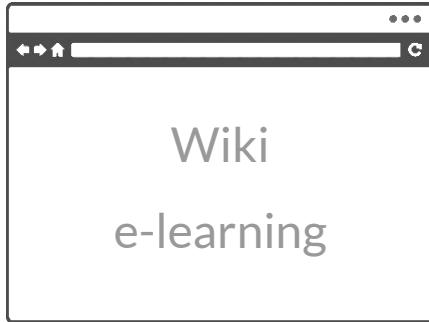


+ Esquema de prioridad basado en peso.




Wiki e-learning

Wiki



- + Contenido con las mejores soluciones
- + Contenido con los lenguajes de la compañía
- + e-learning de seguridad
- + Concientizar y capacitar desarrolladores

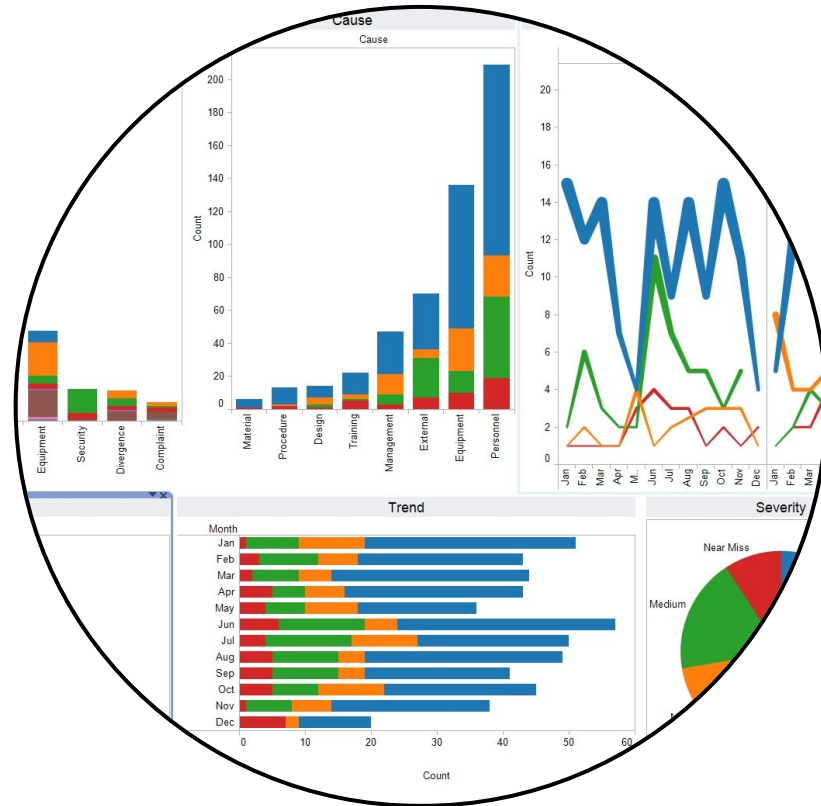


Métricas generales

Metricas



- + Overall risk
- + Vulnerabilidades por proyecto
- + Top 10 Vulnerabilidades más críticas
- + Corregidas vs Reportadas en el tiempo





Evangelizar

- + Trainings presenciales
- + E-learning
- + Competencias internas de seguridad
- + Bug bounties internos
- + Security Focal Points

WE ARE HIRING!

- alejandro.iacobelli@mercadolibre.com
- alexander.campos@mercadolibre.com

