CICLO DE VIDA DEL DESARROLLO DE SOFTWARE SEGURO

@OWASP_Sevilla

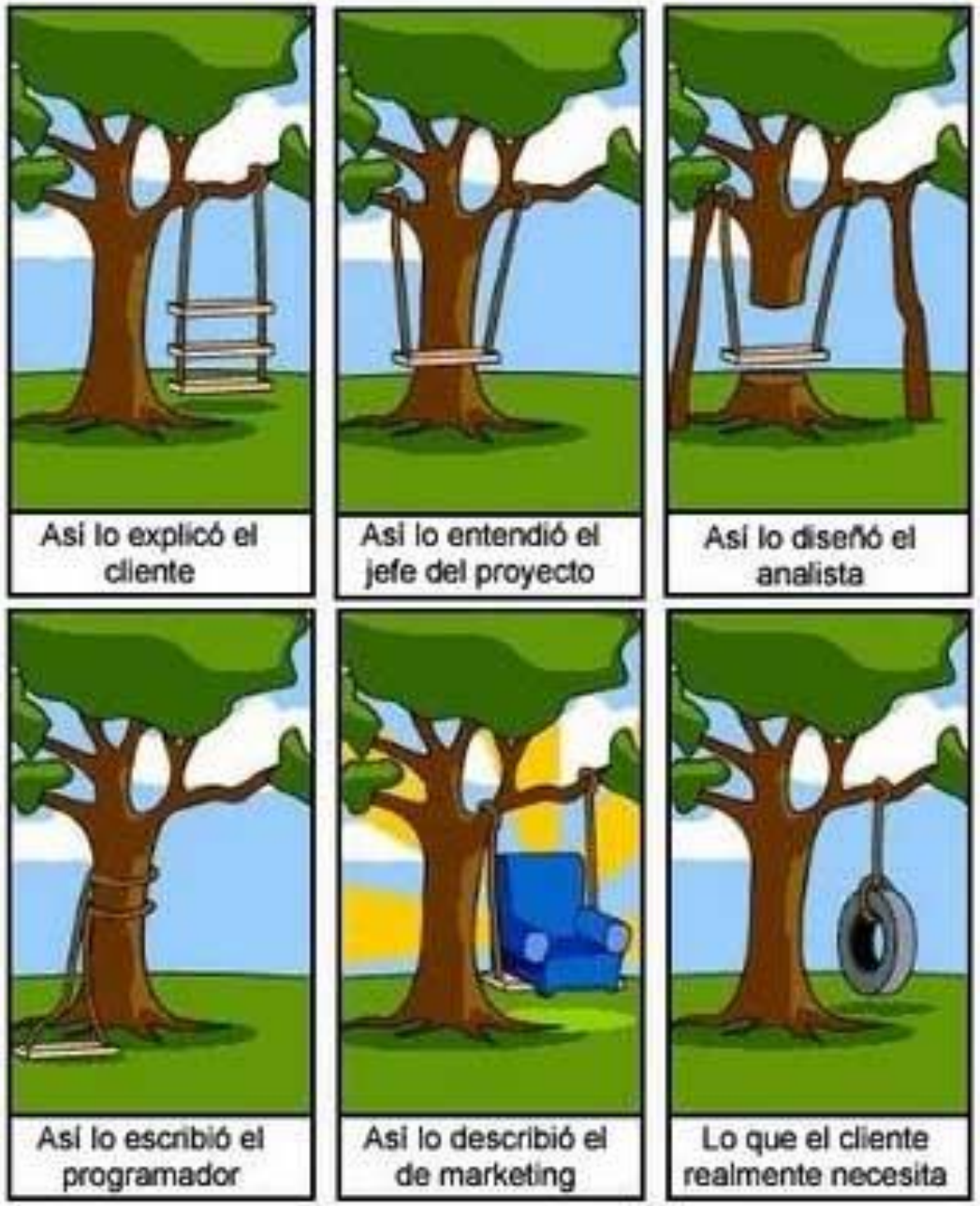
Sevilla CHAPTER

SOBRE MI

Twitter: @juanjodomenech

- Arquitectura y desarrollo software (Seguro)
- Analista en ciberseguridad
- Owasp Sevilla

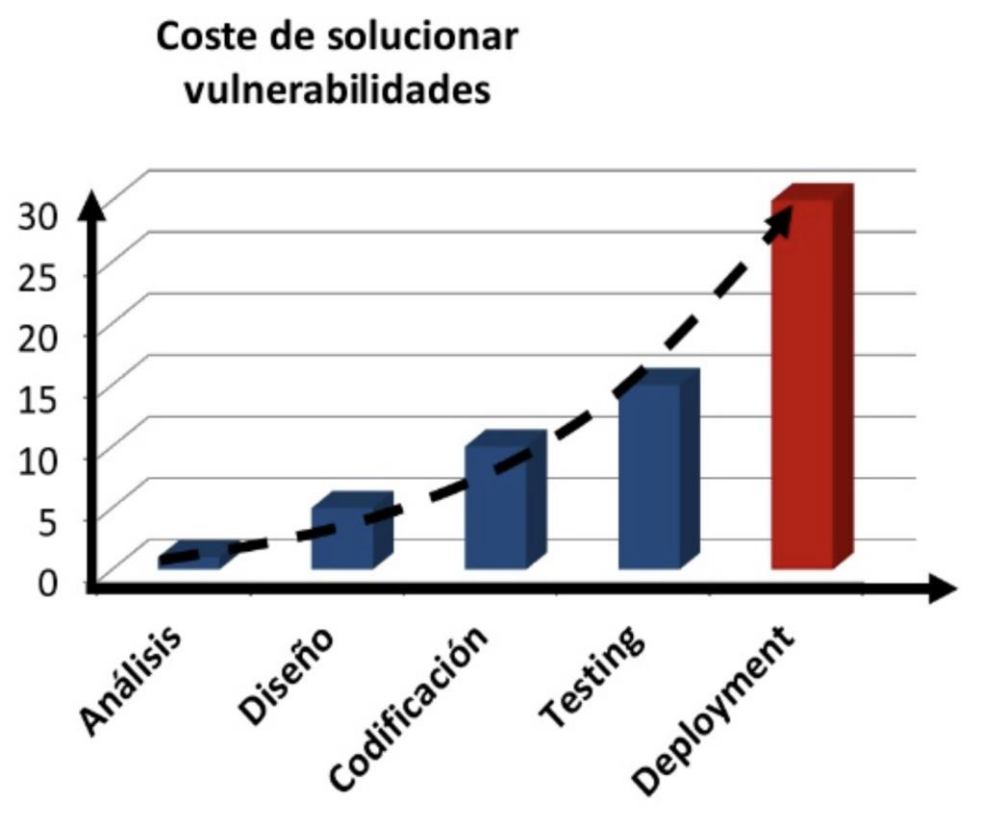
EN MI LOCAL FUNCIONA



QUIÉN ME VA A QUERER HACKEAR

OWASP Top 10 - 2013	→	OWASP Top 10 - 2017
A1 – Injection	→	A1:2017-Injection
A2 – Broken Authentication and Session Management	→	A2:2017-Broken Authentication
A3 – Cross-Site Scripting (XSS)	↘	A3:2017-Sensitive Data Exposure
A4 – Insecure Direct Object References [Merged+A7]	U	A4:2017-XML External Entities (XXE) [NEW]
A5 – Security Misconfiguration	↘	A5:2017-Broken Access Control [Merged]
A6 – Sensitive Data Exposure	↗	A6:2017-Security Misconfiguration
A7 – Missing Function Level Access Contr [Merged+A4]	U	A7:2017-Cross-Site Scripting (XSS)
A8 – Cross-Site Request Forgery (CSRF)	☒	A8:2017-Insecure Deserialization [NEW, Community]
A9 – Using Components with Known Vulnerabilities	→	A9:2017-Using Components with Known Vulnerabilities
A10 – Unvalidated Redirects and Forwards	☒	A10:2017-Insufficient Logging&Monitoring [NEW,Comm.]

BOOOM!



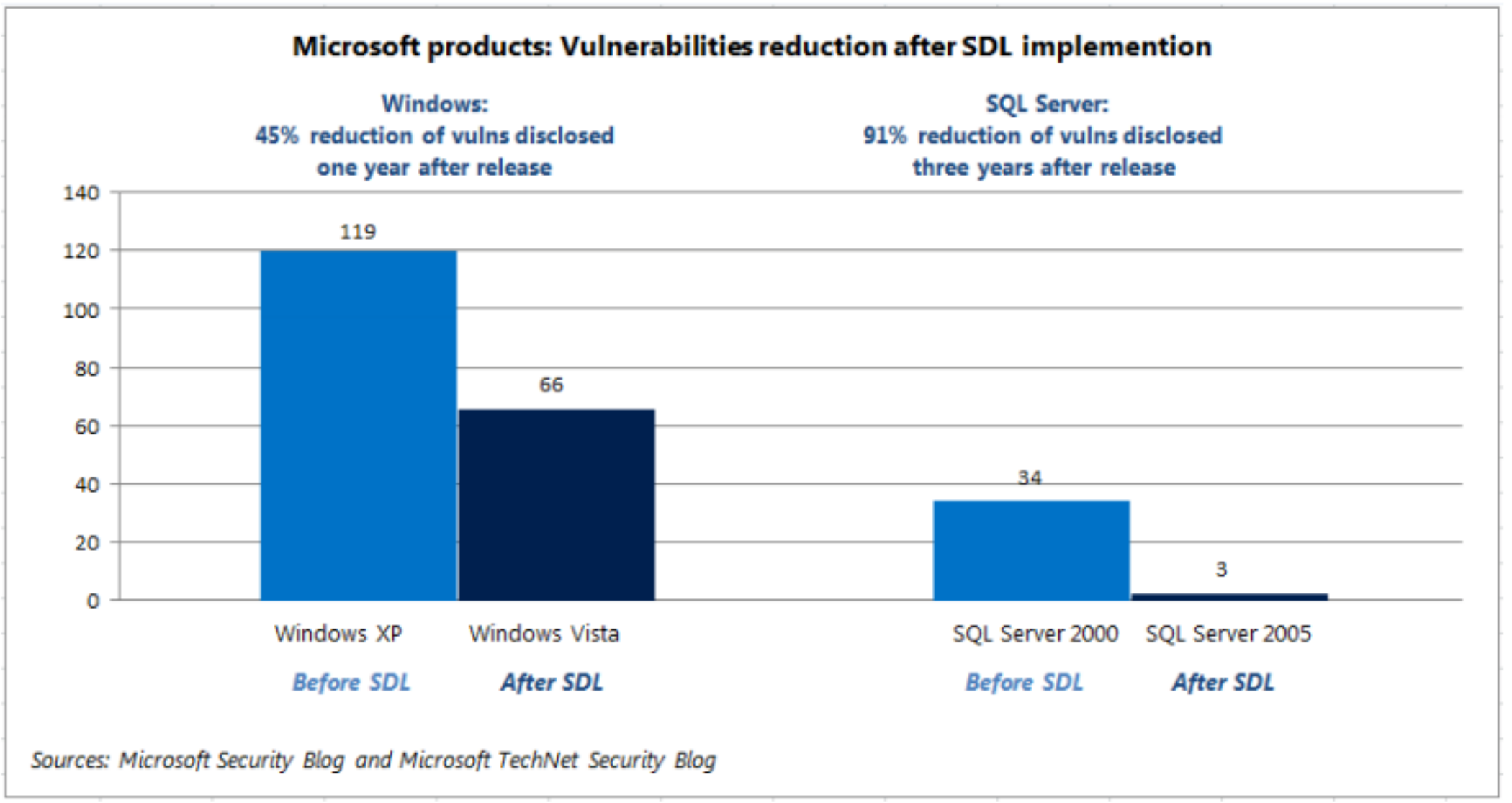
Imágenes de CCN-CERT

SURGE LA NECESIDAD

Modelo de desarrollo seguro (S-SDLC o Ciclo de vida de desarrollo seguro)

- Reducción del número de vulnerabilidades un 40-50%
- Reducción de un 50-70% en constes de gestión de configuración y respuesta a incidentes
- Reducción de un 30% en costes en solucionar el problema
- OJO! Es importante la confianza y privacidad del cliente o usuario final

EJEMPLO


Microsoft products: Vulnerabilities reduction after SDL implemention
Windows:
45% reduction of vulns disclosed
one year after release
SQL Server:
91% reduction of vulns disclosed
three years after release
140
120
100
80
60
40
20
0
119
66
34
3
Windows XP
Windows Vista
SQL Server 2000
SQL Server 2005
Before SDL
After SDL
Before SDL
After SDL
Sources: Microsoft Security Blog and Microsoft TechNet Security Blog

¿POR DONDE EMPIEZO?

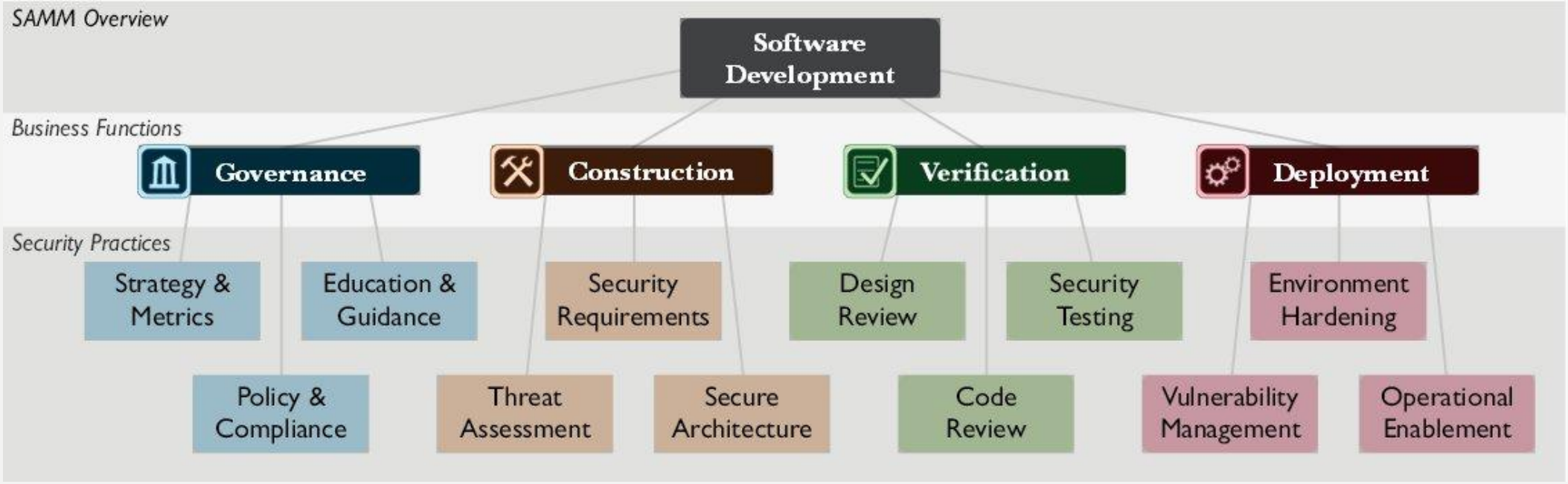
¿POR DONDE EMPIEZO?

METODOLOGÍA DE DESARROLLO SEGURO	EMPRESA	METODOLOGÍA
Microsoft Security Development Lifecycle	Microsoft	Tradicional
Oracle Software Security Assurance	Oracle	Tradicional
Comprehensive Lightweight Application Security Process	OWASP	Tradicional
Team Software Process Secure	Software Engineer Institute	Tradicional
Software Assurance Maturity Model	OWASP	Tradicional
Building Security In Maturity Model	Cigital	Ágil
Agile Development Using Microsoft Security Development Lifecycle	Microsoft	Ágil

METODOLOGÍAS DE SDLC

OWASP
Open Web Application Security Project

OpenSAMM



METODOLOGÍAS DE SDLC

Microsoft®
Security Development Lifecycle

¿CÓMO LO AÑADO EN MI PROYECTO?

¡GRACIAS!