Sécurité Applicative Cheat Sheet

(Franck Jeannot - N420)

Etapes SDL

Security **D**eveloppement **L**ifecycle
7 étapes - 16 activités - 5 parties
Mnemotech : FECIVFR-**VERDICT**

0-Formation (Training)
1-Exigences (Requirements)
2-Conception (Design)
3-Implémentation (Implementation)
4-Vérifications (Verification)
5-Diffusion (Release)
6-Réponse (Response)

Etapes-Activités SDL

Security **D**evelopement **L**ifecycle
7 étapes - 16 activités - 5 parties

0.1 Exigences en formation
1.2 Exigences de sécurité
1.3 Éch. bogues - niv qual.
1.4 An. risq /respect vie priv
2.5 Exigences de conception
2.6 Réd. surface attaque
2.7 Modélisation des menaces
3.8 Utilisation outils approuvés
3.9 Retrait fonctions peu sûres
3.10 Analyse statique
4.11 Analyse dynamique du programme
4.12 Tests inject. fautes aléat.
4.13 Revue surf attaque mod menaces
5.14 Plan de réponse aux incidents
5.15 Analyse finale de la sécurité
5.16 Diffusion/Archivage
6.1 Plan de réponse

Phases Modèle en Cascade

Mnemotech : ACCTVDM - Act V daemon !

Analyse
Conception
Codage
Test
Vérifications
Diffusion
Maintenance

STRIDE

Threat classification model

THREAT	PRO. VIOLATED
Spoofing (imperson.)	Authentication
Tampering (modif. données)	Integrity
Repudiation (répudiation)	Non repudiation
Inf. disclo. (divul. infor)	Confidentiality
Denial of Service (déni services)	Availability
Elevation of Priv. (élév. priv)	Authorization

DREAD

Risk-assessing computer security threats

Damage
Reproducibility
Exploitability
Affected users
Discoverability

Gestion des risques

ISO 27005
menace : cause potentielle d'un incident indésirable, qui peut nuire à un système ou un organisme
Evaluation du risque : Impact X Probabilité

Mod. quantitatif : Single Loss Expectancy (SLE) = valeur d'actif ($) * facteur d'exposition (%)
Facteur d'exposition = pourcentage de perte de l'actif en cas d'incident
Annual Loss Expectancy (ALE) = SLE ARO ARO = Annual rate of occurance
efficacité et la valeur des contrôles : **ROSI** *Return on Security Investment* et RRL
Un contrôle est efficace, si le **RRL** *risk reduction level* **est plus grand que 1**.

Exigences de sécurité

Les exigences de sécurité peuvent être : fonctionnelle, non-fonctionnelle, contrainte,...

Risques

Types : d'affaires, technologique, de non-conformité, informationnel...etc
options avec risques : RMRT : Réduire, Maintenir, Refuser ou Transférer
Menace : Cause potentielle d'un incident indésirable, qui peut nuire à un système ou un organisme.