

# 6 - Sécurité dans les projets

Eléments de cybersécurité d'entreprise

**Yann-Arzel LE VILLIO**

[yannarzel.levillio@orange.com](mailto:yannarzel.levillio@orange.com)

<http://campus.orange.com>

CyberSkills4All  
Direction technique & scientifique OSS

Publication Eléments de cours CYBERSKILLS4ALL

## Abstract



Hashtags : Hardening, ITIL, ANSSI, CSPN

Ce document présente comment différentier la sécurité dans les projets et la sécurité de l'entreprise afin de découvrir les règles techniques de sécurisation des composants du SI, l'organisation des équipes sécurité dans les projets et les enjeux de conformité technique des produits

# Sommaire

1. Introduction
2. Security By Design
3. Règles techniques de sécurisation : durcissement
4. Organisation de la sécurité dans les projets
5. Sécurité des produits



# Sécurité des projets et sécurité d'entreprise



Introduction

Security By  
Design

Règles  
techniques de  
sécurisation :  
durcissement

Organisation de  
la sécurité dans  
les projets

Sécurité des  
produits

Différencier la sécurité dans les projets et la sécurité de l'entreprise

1. security by design
2. les règles techniques de sécurisation des composants du SI
3. organisation des équipes sécurité
4. enjeux de conformité technique des produits

# Minimisation : exemple d'un serveur de Base de données



Introduction

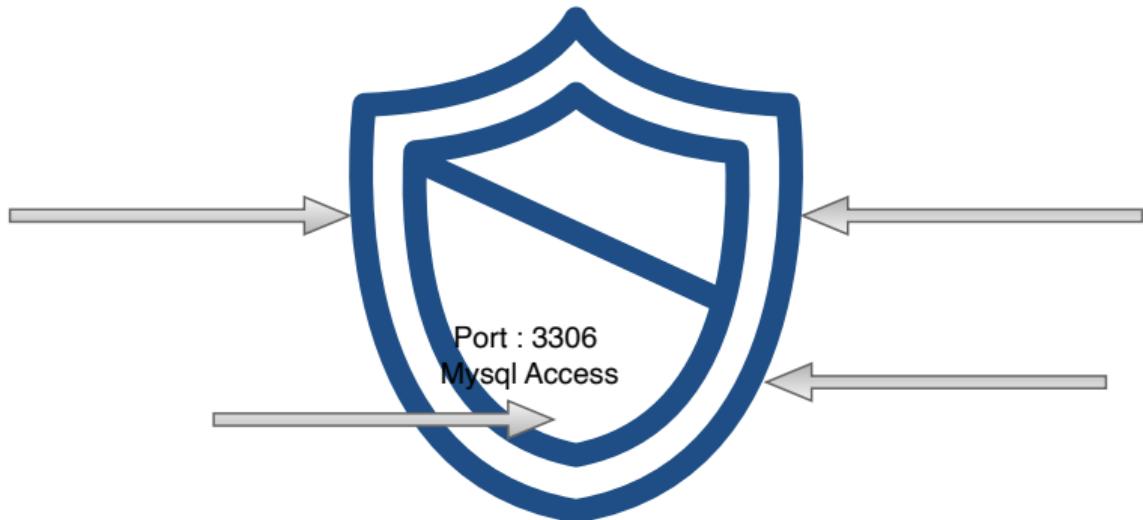
Security By  
Design

Concepts et principes

Règles  
techniques de  
sécurisation :  
durcissement

Organisation de  
la sécurité dans  
les projets

Sécurité des  
produits



Introduction

Security By  
DesignRègles  
techniques de  
sécurisation :  
durcissementOrganisation de  
la sécurité dans  
les projetsSécurité des  
produits

# Security By Design

## # Concepts et principes

- évaluation des risques
- minimisation des surfaces d'attaque
- contrôles de sécurité

## # MCS (Maintien en Condition de Sécurité)

- surveillance continue
- mises à jour
- audits de sécurité
- formation et sensibilisation

## Points à retenir



Introduction

Security By  
Design

Règles  
techniques de  
sécurisation :  
durcissement

Organisation de  
la sécurité dans  
les projets

#

Sécurité des  
produits

#

Introduction

Security By  
DesignRègles  
techniques de  
sécurisation :  
durcissementSécurisation des  
réseauxOrganisation de  
la sécurité dans  
les projetsSécurité des  
produits

# Règles techniques de sécurisation



1. IAM : PKI, MFA, journalisation, contrôles
2. Systèmes d'exploitation et application
3. Matériel (HSM) et locaux (Data Center)
4. Réseaux : VPN, chiffrement, supervision

Introduction

Security By  
DesignRègles  
techniques de  
sécurisation :  
durcissementSécurisation des  
réseauxOrganisation de  
la sécurité dans  
les projetsSécurité des  
produits

# Règles techniques de sécurisation : IAM



- # Public Key Infrastructure (PKI) : pourquoi déployer une infrastructure de gestion de clés ?
- # MFA : Multiple Factor Access
- # journalisation
- # contrôles

# Règles techniques de sécurisation : OS applications : partie 1



Introduction

Security By  
Design

Règles  
techniques de  
sécurisation :  
durcissement

Sécurisation des  
réseaux

Organisation de  
la sécurité dans  
les projets

Sécurité des  
produits

Ref : documents édités par le CIS (Center for Internet Security)

Guide d'hygiène informatique de l'ANSSI

Introduction

Security By  
DesignRègles  
techniques de  
sécurisation :  
durcissementSécurisation des  
réseauxOrganisation de  
la sécurité dans  
les projetsSécurité des  
produits

# Règles techniques de sécurisation : OS Linux



- # Mises à jour régulière
- # Désactiver les services inutiles
- # Configurer un pare-feu
- # Utiliser SELinux (Security Enhanced Linux) ou AppArmor
- # Configurer les permissions des fichiers
- # Désactiver l'accès root à distance
- # Utiliser des clés SSH
- # Installer un logiciel antivirus
- # Configurer les journaux de sécurité
- # Limiter les utilisateurs et groupes
- # Activer le chiffrement des données
- # Configurer des sauvegardes régulières



# Règles techniques de sécurisation : OS Windows

- # Mises à jour régulière
- # Désactiver les services inutiles
- # Configurer un pare-feu
- # Utiliser des comptes utilisateurs standards
- # Activer l'UAC
- # Configurer les stratégies de mot de passe
- # Désactiver l'accès à distance non nécessaire
- # Activer BitLocker
- # Installer un logiciel antivirus
- # Configurer les journaux de sécurité
- # Désactiver SMBv1
- # Limiter les autorisations des applications

Introduction

Security By  
DesignRègles  
techniques de  
sécurisation :  
durcissementSécurisation des  
réseauxOrganisation de  
la sécurité dans  
les projetsSécurité des  
produits

# Règles techniques de sécurisation : applications



Introduction

Security By  
Design

Règles  
techniques de  
sécurisation :  
durcissement

Sécurisation des  
réseaux

Organisation de  
la sécurité dans  
les projets

Sécurité des  
produits

Valable pour toutes applications sur tous les OS!

- # ne pas afficher en accès public la version utilisée
- # règles de design pour protéger les données confidentielles



## Règles techniques de sécurisation : OS applications : partie 2

Ref : documents édités par le CIS (Center for Internet Security)

### # Administration

- Access Control List (ACL) : limiter les accès aux réseaux/utilisateurs dédiés
- réseau admin dédié : séparer les réseaux administration des autres réseaux de l'entreprise
- supervision et administration via réseau chiffré : utilisation de protocoles sécurisés tels que : SNMPv3, SSHv2
- remplacement des mots de passe par défaut par des mots de passe forts
- stockage des mots de passe dans une base de données sécurisée (coffre fort)

### # Exclusion services inutiles : attention aux serveurs web lancés par défaut, etc.

### # Journaux d'événements : garder toutes les traces nécessaires à l'investigation en cas de problème

### # 80 -> 443 : en règle général, préférer les protocoles sécurisés tels que HTTPs, SMTPs, IMAPs, etc.

### # Utilisation de certificats valides

# Règles techniques de sécurisation : Matériel et DC



Introduction

Security By  
Design

Règles  
techniques de  
sécurisation :  
durcissement

Sécurisation des  
réseaux

Organisation de  
la sécurité dans  
les projets

Sécurité des  
produits

- # Chiffrement, zone hardware dédiée (mémoire, voire carte dédiée)
- # HSM
- # Datacenter : salles, contrôles d'accès, caméras, vigiles



## Points à retenir

Introduction

Security By  
Design

Règles  
techniques de  
sécurisation :  
durcissement

Sécurisation des  
réseaux

Organisation de  
la sécurité dans  
les projets

Sécurité des  
produits

# PKI, #CIS, #ACL

# hardening, #HSM

# Organisation de la sécurité dans les projets



Introduction

Security By  
Design

Règles  
techniques de  
sécurisation :  
durcissement

Organisation de  
la sécurité dans  
les projets

Pilotage

Sécurité des  
produits

Quelles sont les missions des équipes sécurité ?

# Ingénierie

# Opération

# Pilotage

Introduction

Security By  
DesignRègles  
techniques de  
sécurisation :  
durcissementOrganisation de  
la sécurité dans  
les projets

Pilotage

Sécurité des  
produits

# Equipe Ingénierie



Quelles sont les missions des équipes ingénierie ?

- # **Analyse des risques**
- # **Normes de développement sécurisé**
- # **Tests de sécurité**
- # **Documentation**

Introduction

Security By  
DesignRègles  
techniques de  
sécurisation :  
durcissementOrganisation de  
la sécurité dans  
les projets

Pilotage

Sécurité des  
produits

# Equipe Opération



Quelles sont les missions des équipes opération ?

- # **Gestion des environnements**
- # **Mises à jour et correctifs**
- # **Surveillance**
- # **Réponse aux incidents**

Introduction

Security By  
DesignRègles  
techniques de  
sécurisation :  
durcissementOrganisation de  
la sécurité dans  
les projets

Pilotage

Sécurité des  
produits

# Equipe Pilotage



Quelles sont les missions des équipes pilotage ?

- # **Coordination**
- # **Indicateurs de performance**
- # **Audits**
- # **Formation et sensibilisation**

Introduction

Security By  
Design

Règles  
techniques de  
sécurisation :  
durcissement

Organisation de  
la sécurité dans  
les projets

Pilotage

Sécurité des  
produits

## Points à retenir

- # #Ingénierie, #opération, #pilotage
- # #OrganisationSécurité



Introduction

Security By  
DesignRègles  
techniques de  
sécurisation :  
durcissementOrganisation de  
la sécurité dans  
les projetsSécurité des  
produits

# Sécurité des produits

La conformité technique aux référentiels et normes permet de garantir que les produits logiciels et matériels répondent aux exigences réglementaires et aux standards de sécurité de l'industrie

But ?

- # valider la robustesse des solutions déployées
- # assurer leur interopérabilité et leur niveau de sécurité
- # mais aussi ...
- # ... un atout concurrentiel!



## Sécurité des produits : Liste référentiels et normes

- # ISO/IEC 27001
- # NIST Cybersecurity Framework (CSF)
- # CIS Controls
- # COBIT
- # PCI DSS
- # GDPR
- # HIPAA
- # SOC 2
- # OWASP Top Ten
- # ITIL
- # SANS Top 20
- # CSA CCM
- # ISO/IEC 27017
- # ISO/IEC 27018
- # ENISA

Introduction

Security By  
DesignRègles  
techniques de  
sécurisation :  
durcissementOrganisation de  
la sécurité dans  
les projetsSécurité des  
produits

## Sécurité des produits : La confiance certifiée

Quel est l'intérêt des certifications CSPN et Critères Communs ?

Pour le vendeur :

- # confiance accrue : la certification CSPN renforce la crédibilité du produit auprès des clients potentiels
- # avantage concurrentiel : se démarquer sur le marché en offrant des produits reconnus pour leur sécurité
- # accès à de nouveaux marchés : facilite l'entrée sur des marchés sensibles où la sécurité est primordiale

Pour l'acheteur :

- # garantie de sécurité : assurance que le produit a été évalué et répond à des normes de sécurité élevées
- # réduction des risques : diminution des vulnérabilités potentielles dans l'infrastructure de l'entreprise
- # conformité réglementaire : aide à respecter les exigences légales et réglementaires en matière de sécurité des systèmes d'information



# Sécurité des produits : CSPN et critères communs



Introduction

Security By  
Design

Règles  
techniques de  
sécurisation :  
durcissement

Organisation de  
la sécurité dans  
les projets

Sécurité des  
produits

- # Certification de Sécurité de Premier Niveau (CSPN) : tests en « boîte noire »
  - > Exemples : Harfanglab EDR et Stormshield security (poste de travail)
- # critères communs : certification qui permet à un client de s'assurer par l'intervention organisme certificateur, de la conformité d'un produit à un cahier des charges ou à une spécification technique
  - > Exemples : Les produits Zed! et ZoneCentral de PRIM'X



## Points à retenir

Introduction

Security By  
Design

Règles  
techniques de  
sécurisation :  
durcissement

Organisation de  
la sécurité dans  
les projets

Sécurité des  
produits

- # Conformité == répondre aux exigences réglementaires et aux standards de sécurité de l'industrie
  - > #ISO/IEC 27001 #NIST #CIS Controls #COBIT #PCI DSS #GDPR -> #HIPAA #SOC 2 #OWASP Top Ten #ITIL #SANS Top20 #CSA CCM -> #ISO/IEC 27017 #ISO/IEC 27018 #ENISA
- # La confiance certifié
  - > #CSPN #Critères Communs



**des questions ?**

## Contributions



Les notes et les présentations sont réalisées sous  $\text{\LaTeX}$ .

Vous pouvez contribuer au projet du cours CYBERDEF101. Les contributions peuvent se faire sous deux formes :

- # Corriger, amender, améliorer les notes publiées. A chaque session des modifications et évolutions sont apportées pour tenir compte des corrections de fond et de formes.
- # Ajouter, compléter, modifier des parties de notes sur la base de votre lecture du cours et de vos expertises dans chacun des domaines évoqués.

Les fichiers sources sont publiés sur GITHUB dans l'espace :

(edufaction/CYBERDEF101) ↗<sup>a</sup>.

---

a. <https://github.com/edufaction/CYBERDEF101>

## Mises à jour régulières

Vérifiez la disponibilité d'une version plus récente de

[L-Orange-Cyberdef101-M6c-Secuprojet.przt.pdf sur GITHUB CYBERDEF ↗<sup>1</sup>](#)



2025 eduf@ction - Publication en Creative Common BY-NC-ND

