

6 - Sécurité dans les projets

Eléments de cybersécurité d'entreprise

Yann-Arzel LE VILLIO

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 différencier 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 Product
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

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

Introduction

Product

Security By

Design

Règles
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

Product

Security By

Design

Règles
techniques de
sécurisation :
durcissement

Organisation de
la sécurité dans
les projets

#

#

Sécurité des
produits

Introduction

Product

Security By

Design

Règles
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



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

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

Hardening OS

- UNIX/LINUX : SELinux
- WINDOWS : GPO, Applocker

Applications :

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

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, SSH
- 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,

Règles techniques de sécurisation : Matériel et DC



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

Introduction

Product

Security By

Design

Règles
techniques de
sécurisation :
durcissement

Sécurisation des
réseaux

Organisation de
la sécurité dans
les projets

Sécurité des
produits

Points à retenir

- # #PKI, #CIS, #ACL
- # #hardening, #HSM



Introduction

Product

Security By

Design

Règles
techniques de
sécurisation :
durcissementOrganisation de
la sécurité dans
les projets

Pilotage

Sécurité des
produits

Organisation de la sécurité dans les projets



Quelles sont les missions des équipes sécurité ?

- # Ingénierie
- # Opération
- # Pilotage

Introduction

Product

Security By

Design

Règles
techniques de
sécurisation :
durcissement

Organisation de
la sécurité dans
les projets

Pilotage

Sécurité des
produits

Equipe Ingénierie



Analyse des risques

Normes de développement sécurisé

Tests de sécurité

Documentation

Introduction

Product

Security By

Design

Règles
techniques de
sécurisation :
durcissement

Organisation de
la sécurité dans
les projets

Pilotage

Sécurité des
produits

Equipe Opération



Gestion des environnements

Mises à jour et correctifs

Surveillance

Réponse aux incidents

Introduction

Product

Security By

Design

Règles
techniques de
sécurisation :
durcissement

Organisation de
la sécurité dans
les projets

Pilotage

Sécurité des
produits

Equipe Pilotage



Coordination

Indicateurs de performance

Audits

Formation et sensibilisation



Points à retenir

Introduction

Product

Security By

Design

Règles
techniques de
sécurisation :
durcissement

Organisation de
la sécurité dans
les projets

Pilotage

Sécurité des
produits

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

Introduction

Product

Security By

Design

Règles
techniques de
sécurisation :
durcissement

Organisation de
la sécurité dans
les projets

Sécurité des
produits

Sécurité des produits



Protocoles réseaux

Normes environnementales



Sécurité des produits

- # Certification de Sécurité de Premier Niveau (CSPN) : tests en « boîte noire »
- # critères communs : certification qui permet à un client de s'assurer par l'intervention d'un organisme certificateur, de la conformité d'un produit à un cahier des charges ou à une spécification technique



Points à retenir

Introduction

Product

Security By

Design

Règles
techniques de
sécurisation :
durcissement

Organisation de
la sécurité dans
les projets

#

#

Sécurité des
produits



des questions ?

Contributions



Les notes et les présentations sont réalisées sous \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) ↗^a.

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 ↗¹](#)



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

