

6 - Sécurité dans les projets

Éléments de cybersécurité d'entreprise

Yann-Arzel LE VILLIO

yann-arzel.levillio@orange.com

<http://campus.orange.com>

Orange CyberSchool
Direction technique & scientifique

Publication Éléments de cours CYBERSKILLS4ALL



CYBERDEF 101

Éléments de cybersécurité
et de cyberdéfense
d'entreprise



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. Règles techniques de sécurisation /
durcissement

3. Organisation de la sécurité dans les
projets

4. Sécurité des produits



Sécurité des projets et sécurité d'entreprise



Introduction

Product

Règles

techniques de
sécurisation /
durcissement

Organisation de
la sécurité dans
les projets

Sécurité des
produits

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

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

Règles techniques de sécurisation



Introduction

Product

Règles
techniques de
sécurisation /
durcissement

Réseaux

Organisation de
la sécurité dans
les projets

Sécurité des
produits

1. IAM
2. Systèmes d'exploitation
3. Matériel et Locaux (Data Center)
4. Réseaux : VPN, chiffrement

Règles techniques de sécurisation : IAM



Introduction

Product

Règles
techniques de
sécurisation /
durcissement

Réseaux

Organisation de
la sécurité dans
les projets

Sécurité des
produits

- # 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 générale, préférer les protocoles sécurisés tels que HTTPS,

Règles techniques de sécurisation : Matériel et DC



Introduction

Product

Règles
techniques de
sécurisation /
durcissement

Réseaux

Organisation de
la sécurité dans
les projets

Sécurité des
produits

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

Points à retenir



Introduction

Product

Règles
techniques de
sécurisation /
durcissement

Réseaux

Organisation de
la sécurité dans
les projets

Sécurité des
produits

#CIS, #ACL

#hardening, #HSM,

Organisation de la sécurité dans les projets



Introduction
Product

Règles
techniques de
sécurisation /
durcissement

Organisation de
la sécurité dans
les projets

Sécurité des
produits

Ingénierie : missions

Opération : missions

Pilotage : missions

Points à retenir



Introduction

Product

Règles
techniques de
sécurisation /
durcissement

Organisation de
la sécurité dans
les projets

#

Sécurité des
produits

#

Sécurité des produits



Introduction

Product

Règles
techniques de
sécurisation /
durcissement

Organisation de
la sécurité dans
les projets

Sécurité des
produits

Protocoles réseaux

Normes environnementales

Sécurité des produits



Introduction

Product

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 »
- # 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

Points à retenir



Introduction

Product

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](https://github.com/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



2024 eduf@ction - Publication en Creative Common BY-NC-ND



CYBERDEF 101

Eléments de cybersécurité
et de cyberdéfense
d'entreprise

