

3 - Architectures, Composants et Sécurité

Eléments de cybersécurité d'entreprise

Yann-Arzel LE VILLIO

yann-arzel.levillio@orange.com

<http://campus.orange.com>

Orange CyberSchool
Direction technique & scientifique

Publication Eléments de cours CYBERSKILLS4ALL



CYBERDEF 101
Eléments de cybersécurité
et de cyberdéfense
d'entreprise



Abstract



Hashtags : Architectures, composants sécurité, SSI

Ce document présente les architectures, Composants de cybersécurité.

Sommaire

1. Introduction Architecture
2. De l'analyse de risques aux fonctions de sécurité
3. Architecture et composants de système d'information
4. Modèles de sécurité et technologies de sécurité protectrices
5. Sécurité Endpoints





Architectures, Composants et Sécurité

Introduction
Architecture

De l'analyse de
risques aux
fonctions de
sécurité

Architecture et
composants de
système
d'information

Modèles de
sécurité et
technologies de
sécurité
protectrices

Sécurité
Endpoints

Construire une architecture sécurisée : politique, sécurité des solutions,
identification des composants

1. De l'analyse de risques aux fonctions de sécurité
2. Architecture et composants de système d'information
3. Modèles de sécurité et technologies de sécurité protectrices
4. Sécurité Endpoints

De l'analyse de risques aux fonctions de sécurité



Introduction
Architecture

De l'analyse de
risques aux
fonctions de
sécurité

Architecture et
composants de
système
d'information

Modèles de
sécurité et
technologies de
sécurité
protectrices

Sécurité
Endpoints

1. Filtrage : cloisonnement, Multitenant
2. Accès : RBAC (Role Based Access Control), droit d'en connaître
3. Cryptographie : intégrité des données, protection des flux (IPSec, VPN SSL)



Cloisonnement

Introduction
Architecture

De l'analyse de
risques aux
fonctions de
sécurité

Filtrage

Architecture et
composants de
système
d'information

Modèles de
sécurité et
technologies de
sécurité
protectrices

Sécurité
Endpoints

-> isoler les zones entre elles en fonction :

- # des groupes, utilisateurs et clients (Multitenant)
- # des services et exposition (Internet, Intranet/internes, etc.)
- # des zones d'exploitation : production, tests ou entraînements

! Attention de contrôler les flux entre les zones...

Gestion des identités : IAM



Introduction
Architecture

De l'analyse de
risques aux
fonctions de
sécurité

Accès

Architecture et
composants de
système
d'information

Modèles de
sécurité et
technologies de
sécurité
protectrices

Sécurité
Endpoints

Définition

- IAM (identity and access management) Gestion des Identités et des Accès
- PAM (privileged access management) Gestion des comptes à privilèges , centralise la gestion des profils d'administrateur et assure que l'accès au moindre privilège est appliqué pour donner aux utilisateurs uniquement l'accès dont ils ont besoin.

Process Gestion des identités - cycle de vie

Procédures Contrôle des habilitations

Gestion des identités : IAM



Introduction
Architecture

De l'analyse de
risques aux
fonctions de
sécurité

Accès

Architecture et
composants de
système
d'information

Modèles de
sécurité et
technologies de
sécurité
protectrices

Sécurité
Endpoints

- # Processus de gestion des identifiants, arrivées, départs, demandes d'habilitations, etc.
- # Politique de contrôle des accès : certificats, authentification multifacteurs (MFA)
- # IAG (identity access governance) automatise la création, la gestion et la certification des comptes d'utilisateurs, des rôles et des droits d'accès pour les utilisateurs provisionnement des utilisateurs, gestion des mots de passe, gestion des politiques, gouvernance des accès et revue des accès

Gestion des identités : PAM



Introduction
Architecture

De l'analyse de
risques aux
fonctions de
sécurité

Accès

Architecture et
composants de
système
d'information

Modèles de
sécurité et
technologies de
sécurité
protectrices

Sécurité
Endpoints

PAM (privileged access management) Gestion des comptes à privilèges, centralise la gestion des profils d'administrateur et assure que l'accès au moindre privilège est appliqué pour donner aux utilisateurs uniquement l'accès dont ils ont besoin.

Cryptographie



Introduction
Architecture

De l'analyse de
risques aux
fonctions de
sécurité

Accès

Architecture et
composants de
système
d'information

Modèles de
sécurité et
technologies de
sécurité
protectrices

Sécurité
Endpoints

Cryptologie : science du secret

Algorithmes

- Chiffrement à clefs secrètes
- Cryptographie à clefs publiques
- Fonction de hachage
- Clefs

Cryptographie



Introduction
Architecture

De l'analyse de
risques aux
fonctions de
sécurité

Accès

Architecture et
composants de
système
d'information

Modèles de
sécurité et
technologies de
sécurité
protectrices

Sécurité
Endpoints

- # Taille de clefs : 2048 bits
- # Aléas et générateur d'aléas
- # Protocoles et formats
- # Certificats auto-signés
- # IGC (infrastructure de gestion de clefs) ou PKI (public key infrastructure)

Cryptographie



Introduction
Architecture

De l'analyse de
risques aux
fonctions de
sécurité

Accès

Architecture et
composants de
système
d'information

Modèles de
sécurité et
technologies de
sécurité
protectrices

Sécurité
Endpoints

- # pour les équipes réseaux : tunnels IPSEC, VPNSL, chiffreurs réseaux
- # pour les équipes des services informatiques : le déploiement, la mise à jour des certificats sur des terminaux et des serveurs concentrent une bonne partie des problèmes opérationnels
- # pour la bureautique et le poste de travail : les produits et les services pour chiffrer les données et préserver la confidentialité dans les messageries ou sur les supports (smartdevice, disques, USB, serveur de fichiers) sont complexes à choisir pour l'interopérabilité;
- # pour les métiers de l'entreprise comme les achats ou l'archivage probant, les enjeux d'authenticité, d'imputabilité et d'intégrité ainsi que la signature électronique nécessitent des travaux transverses à l'entreprise souvent coûteux.



Cryptographie

Introduction
Architecture

De l'analyse de
risques aux
fonctions de
sécurité

Accès

Architecture et
composants de
système
d'information

Modèles de
sécurité et
technologies de
sécurité
protectrices

Sécurité
Endpoints

Usure ou rupture cryptographique : la cryptographie quantique, quels sont les nouveautés et les risques ?

- rupture de la sécurité de la cryptographie classique
- compromission de la confidentialité des communications

Blockchain, Crypto-monnaies, NFT (Non-Fungible Tokens)

Architecture et composants de système d'information



1. Architectures logicielles - Monolithe vs microservices
 - FrontEnd : Web, applications mobiles, clientless
 - Backend
 - Bases de données
2. Middleware : Messagerie, ERP
3. Endpoints : PC, mobile, IoT
4. Réseau : traçabilité de tt accès, transactions et anomalies (bugs, erreurs, détection)

Modèles de sécurité et technologies de sécurité protectrices



Introduction
Architecture

De l'analyse de
risques aux
fonctions de
sécurité

Architecture et
composants de
système
d'information

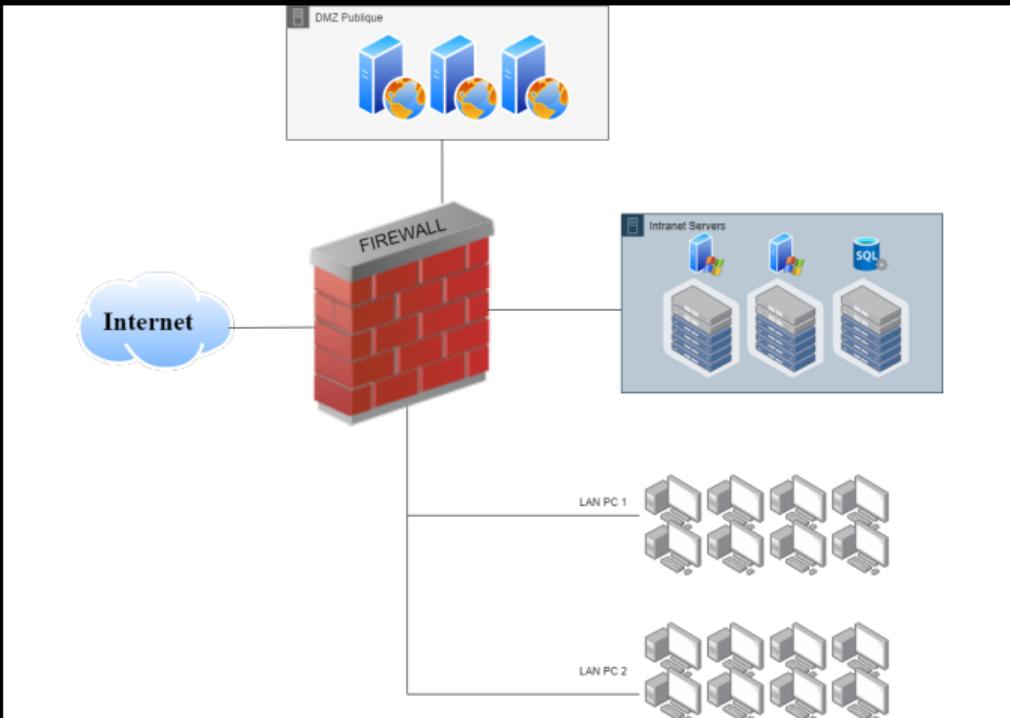
Modèles de
sécurité et
technologies de
sécurité
protectrices

Sécurité
Endpoints

Depuis le modèle du château fort jusqu'aux solutions de sécurité utilisées dans les déploiements CLOUD

**#Firewall #Proxy #ReverseProxy #IDS/IDP #ZeroTrust #Bastion #VPN #CASB
#SASE**

Château fort



Firewall



- # Fonctions sécurité : filtrage et cloisonnement
- # Le pare feu empêche et jette les flux illégitimes
- # Seuls ceux autorisés sont routés vers les destinations

Proxy



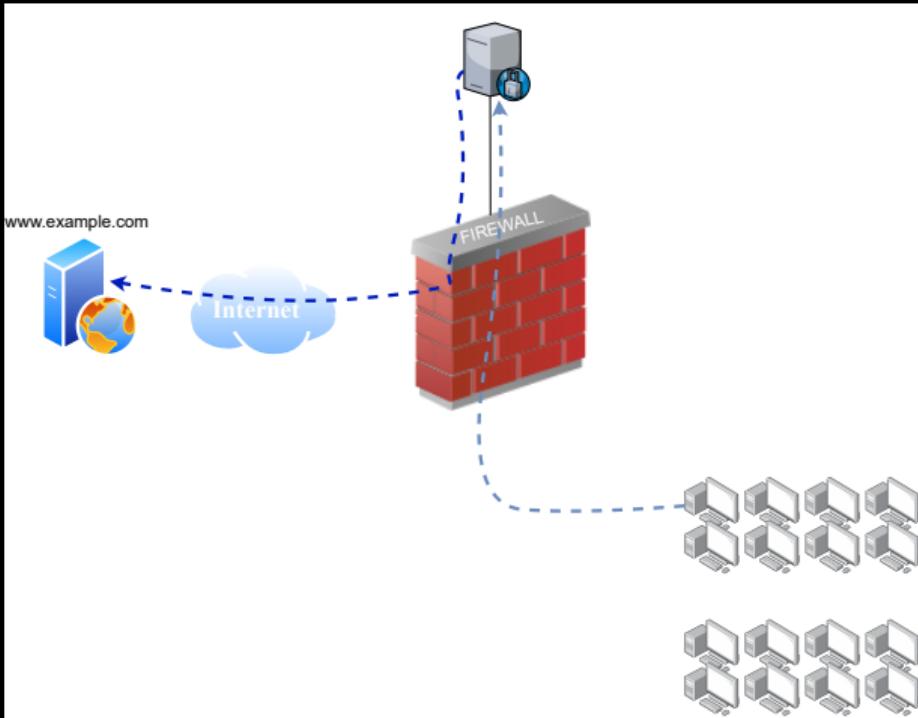
Introduction
Architecture

De l'analyse de
risques aux
fonctions de
sécurité

Architecture et
composants de
système
d'information

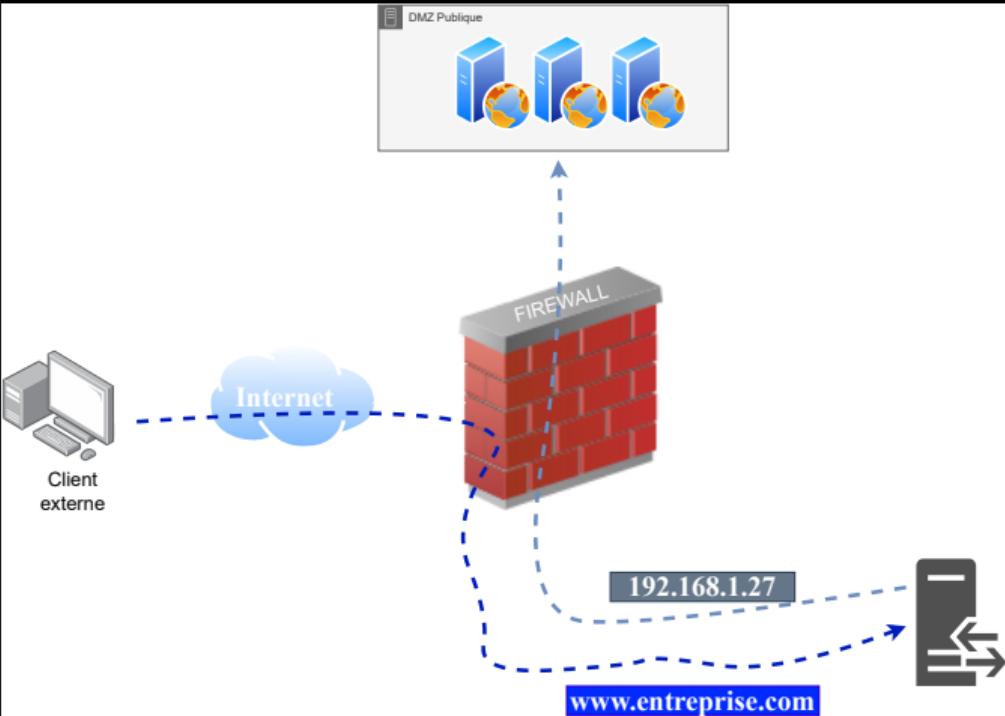
Modèles de
sécurité et
technologies de
sécurité
protectrices

Sécurité
Endpoints





ReverseProxy



Introduction
Architecture

De l'analyse de
risques aux
fonctions de
sécurité

Architecture et
composants de
système
d'information

Modèles de
sécurité et
technologies de
sécurité
protectrices

Sécurité
Endpoints



IDS/IDP

Introduction
Architecture

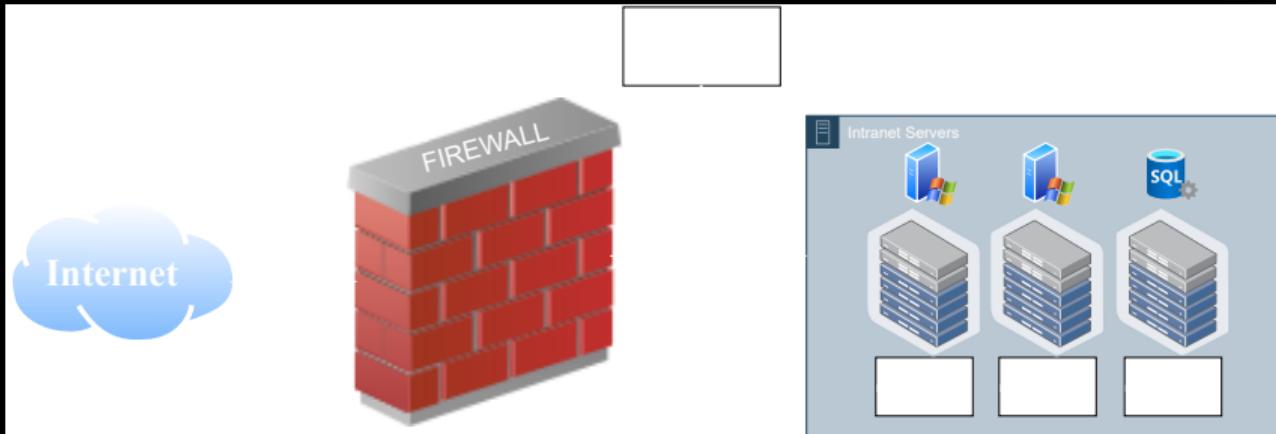
De l'analyse de
risques aux
fonctions de
sécurité

Architecture et
composants de
système
d'information

Modèles de
sécurité et
technologies de
sécurité
protectrices

Sondes de détection
(IDS/IDP)

Sécurité
Endpoints





Zerotrust

Introduction
Architecture

De l'analyse de
risques aux
fonctions de
sécurité

Architecture et
composants de
système
d'information

Modèles de
sécurité et
technologies de
sécurité
protectrices

Sécurité
Endpoints

Limites du modèle de sécurité périphérique : télétravail, Cloud, BYOD ->
réduction du contrôle VS augmentation de la menace

Le modèle impose :

- une réduction de la confiance implicite aux utilisateurs
- ajout de contrôles et de politique d'accès aux ressources

Introduction
ArchitectureDe l'analyse de
risques aux
fonctions de
sécuritéArchitecture et
composants de
système
d'informationModèles de
sécurité et
technologies de
sécurité
protectricesSécurité
Endpoints

Les actions d'administration imposent entre autres des exigences de traçabilité et de confidentialité. La figure ci-dessous présente la mise en œuvre de rebonds dans une zone d'administration permettant d'appliquer un certain nombre de traitements tels le filtrage des connexions, l'authentification des administrateurs sur un portail frontal, un contrôle d'accès ou encore la journalisation des actions effectuées et des commandes exécutées par les administrateurs. Le bastion constitue une ressource d'administration critique dans la mesure où il concentre potentiellement à un instant des secrets d'authentification des comptes d'administration ou des journaux liés aux actions d'administration. Il ne doit donc pas être exposé sur un SI de faible niveau de confiance, un SI bureautique par exemple.

ANSSI (AGENCE NATIONALE SÉCURITÉ DES SYSTÈMES D'INFORMATION)*RECOMMANDATIONS RELATIVES À L'ADMINISTRATION SÉCURISÉE DES SYSTÈMES D'INFORMATION v3-0*



Bastion

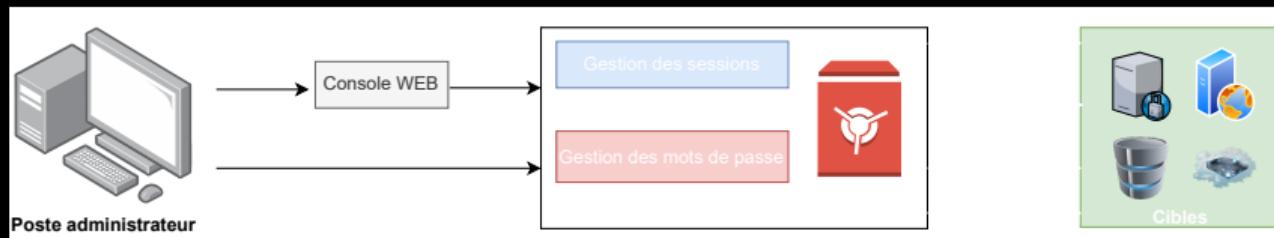
Introduction
Architecture

De l'analyse de
risques aux
fonctions de
sécurité

Architecture et
composants de
système
d'information

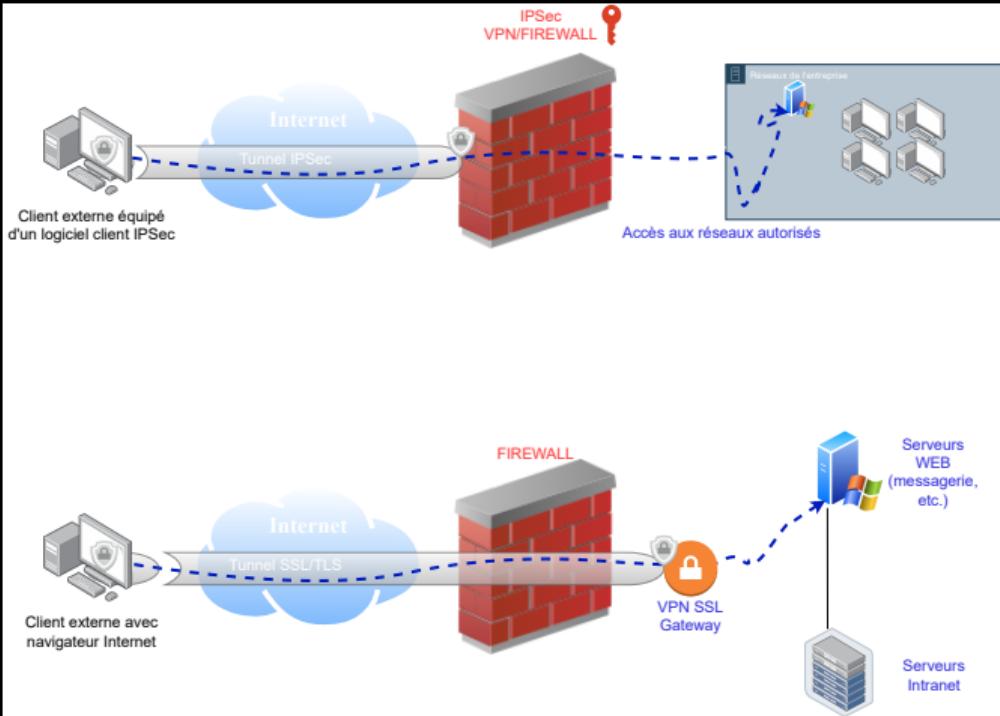
Modèles de
sécurité et
technologies de
sécurité
protectrices

Sécurité
Endpoints





VPN IPSec vs VPN SSL



Cloud



Introduction
Architecture

De l'analyse de
risques aux
fonctions de
sécurité

Architecture et
composants de
système
d'information

Modèles de
sécurité et
technologies de
sécurité
protectrices

Sécurité
Endpoints

- # MultiCloud : double déploiement sur des CSP
- # CloudHybride : Master sur Cloud Publique et Slave sur Cloud Privé

Introduction
Architecture

De l'analyse de
risques aux
fonctions de
sécurité

Architecture et
composants de
système
d'information

Modèles de
sécurité et
technologies de
sécurité
protectrices

Sécurité
Endpoints

Cloud Access Security Broker - CASB



- # But : protéger et surveiller les applications dans le CLOUD
- # Fonctionnalités : Authentification, chiffrement, DLP, mapping des identifiants, etc.
- # Schéma ?



Secure access service edge (SASE)

Introduction
Architecture

De l'analyse de
risques aux
fonctions de
sécurité

Architecture et
composants de
système
d'information

Modèles de
sécurité et
technologies de
sécurité
protectrices

Sécurité
Endpoints

fonctionnalités réseau et sécurité, dans un environnement Cloud Natif incluant les technologies/services Cloud Based suivants :

- # SD-WAN (Software Defined WAN)
- # SWG (Proxy sortant sécurisé)
- # CASB (Cloud Access Security Broker)
- # NGFW (firewalls de nouvelle génération)
- # zero trust network access (ZTNA)

Points à retenir



Introduction
Architecture

De l'analyse de
risques aux
fonctions de
sécurité

Architecture et
composants de
système
d'information

Modèles de
sécurité et
technologies de
sécurité
protectrices

Sécurité
Endpoints

- # Le modèle du château fort demeure mais évolue
- # les technologies de protection et filtrage évoluent et restent indispensables à la SSI
 - > #FirewallNextGeneration #ProxydansleCloud
- # les contrôles d'accès administrateurs et utilisateurs sont de plus en plus fins et imposent une rigueur d'implémentation et de gestion dans le temps
 - > #Bastion #ZeroTrust
- # La sécurité périmétrique s'étend jusqu'au Cloud
 - > #CASB #SASE

Sécurité Endpoints



- # Antivirus classique et NGAV (Next Gen Antivirus)
- # Endpoint Detection and Response : EDR
 - Déetecter les incidents de sécurité
 - Contenir l'incident au point final
 - Enquêter sur les incidents de sécurité
 - Fournir des conseils de remédiation
- # eXtended Detection and Response : XDR corrélation et analyse des données des endpoints, des éléments déployés dans le cloud, des réseaux et de la messagerie



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 :
<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-M3c-Architectures.przt.pdf sur GITHUB CYBERDEF 



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



CYBERDEF 101
Eléments de cybersécurité
et de cyberdéfense
d'entreprise