

# 3 - Architectures, Composants et Sécurité

Eléments de cybersécurité d'entreprise

**Yann-Arzel LE VILLIO**

[yann-arzel.levillio@orange.com](mailto:yann-arzel.levillio@orange.com)

<http://campus.orange.com>

Orange CyberSchool  
Direction technique & scientifique

Publication Eléments de cours CYBERSKILLS4ALL



# Abstract



Hashtags : Architectures, composants sécurité, SSI

Ce document présente les architectures, Composants de cybersécurité.

# Sommaire

Introduction Architecture

De l'analyse de risques aux fonctions  
de sécurité

Architecture et composants de  
système d'information

Introduction

Château fort

6. pare-feu

Proxy

Sondes de détection (IDS/IDP)

Network Access Control : NAC

Zero Trust

Bastion

VPN

Cloud

Cloud Access Security Broker - CASB

Secure access service edge (SASE)





# Architectures, Composants et Sécurité

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

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

# De l'analyse de risques aux fonctions de sécurité



Filtrage : cloisonnement, Multitenant

Accès : RBAC (Role Based Access Control), droit d'en connaître

Cryptographie : intégrité des données, protection des flux (IPSec, VPN SSL)



## Cloisonnement

Filtrage

-> 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

Accès

## # 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

Accès

- # 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

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.

# Cryptographie



Accès

# Cryptologie : science du secret

# Algorithmes

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

# Cryptographie



Accès

- # 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

Accès

- # pour les équipes réseaux : tunnels IPSEC, VPNSSL, 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

Accès

- # 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

## Architectures logicielles - Monolithe vs microservices

- FrontEnd : Web, applications mobiles, clientless
- Backend
- Bases de données

Middleware : Messagerie, ERP

Endpoints : PC, mobile, IoT

Réseau : traçabilité de tt accès, transactions et anomalies (bugs, erreurs, détection)

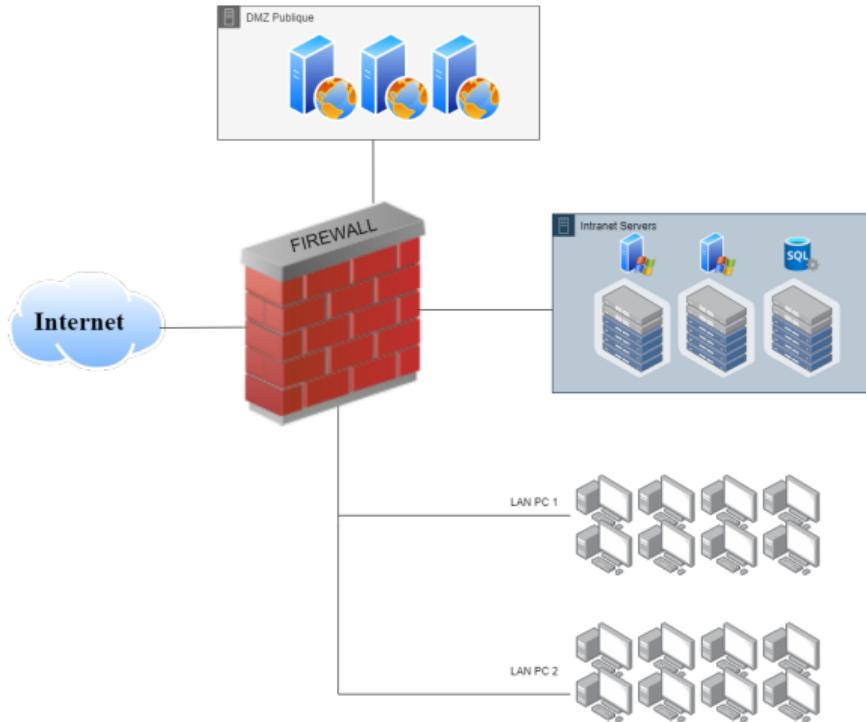
# Modèles de sécurité et technologies de sécurité protectrices



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

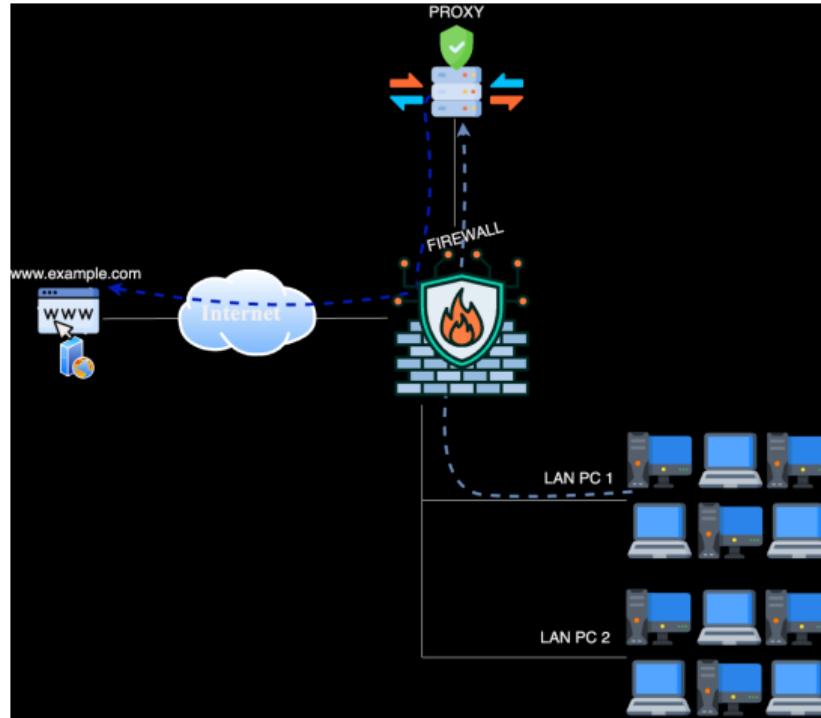


# Firewall



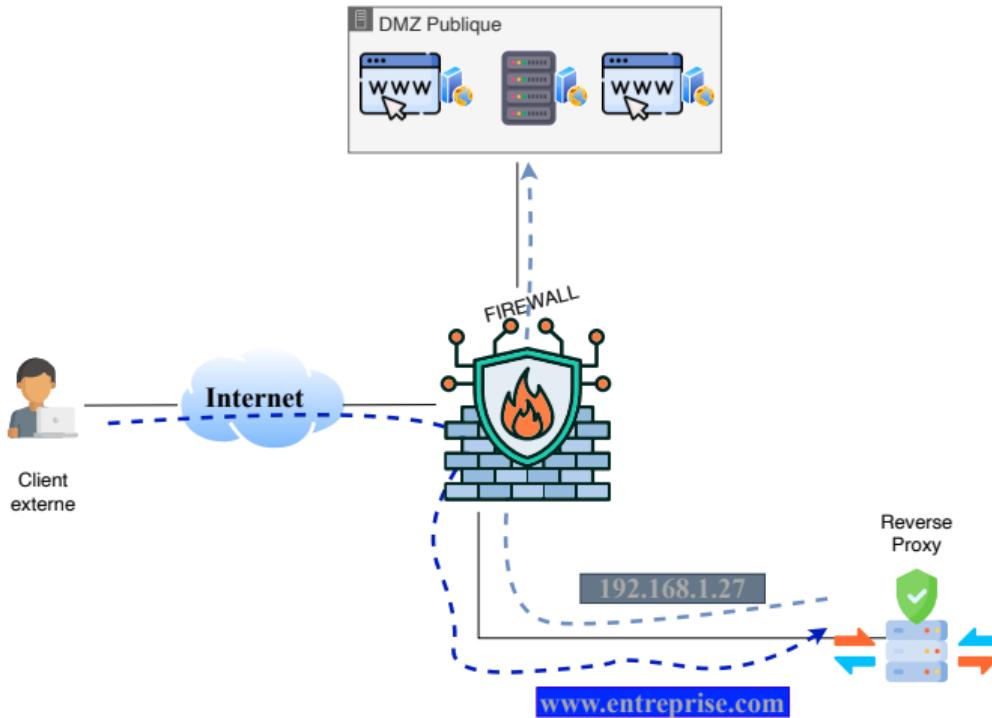
- # Fonctions sécurité : filtrage et cloisonnement
- # Le pare feu empêche et jette les flux illégitimes
- # Seuls ceux autorisés sont routés vers les destinations

# Proxy

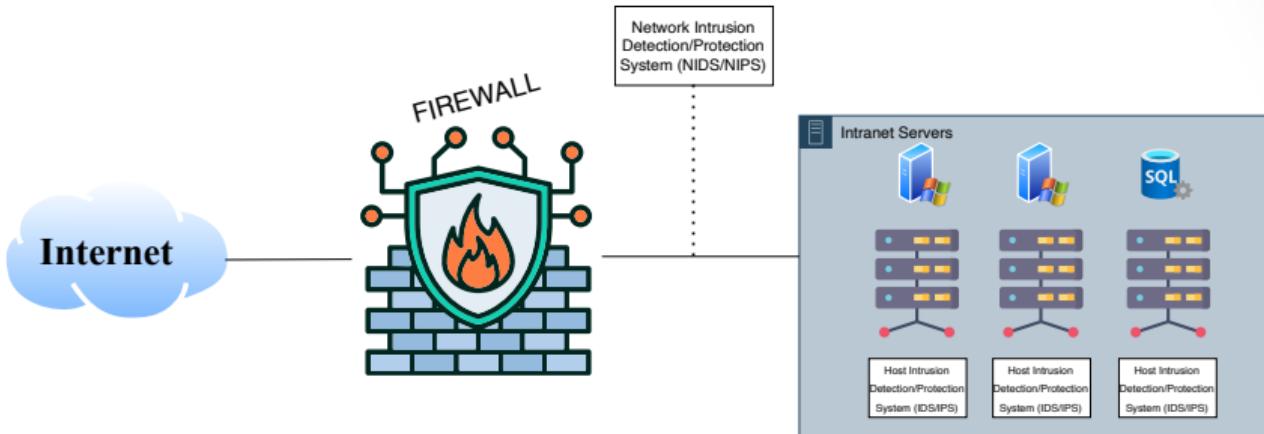




# ReverseProxy

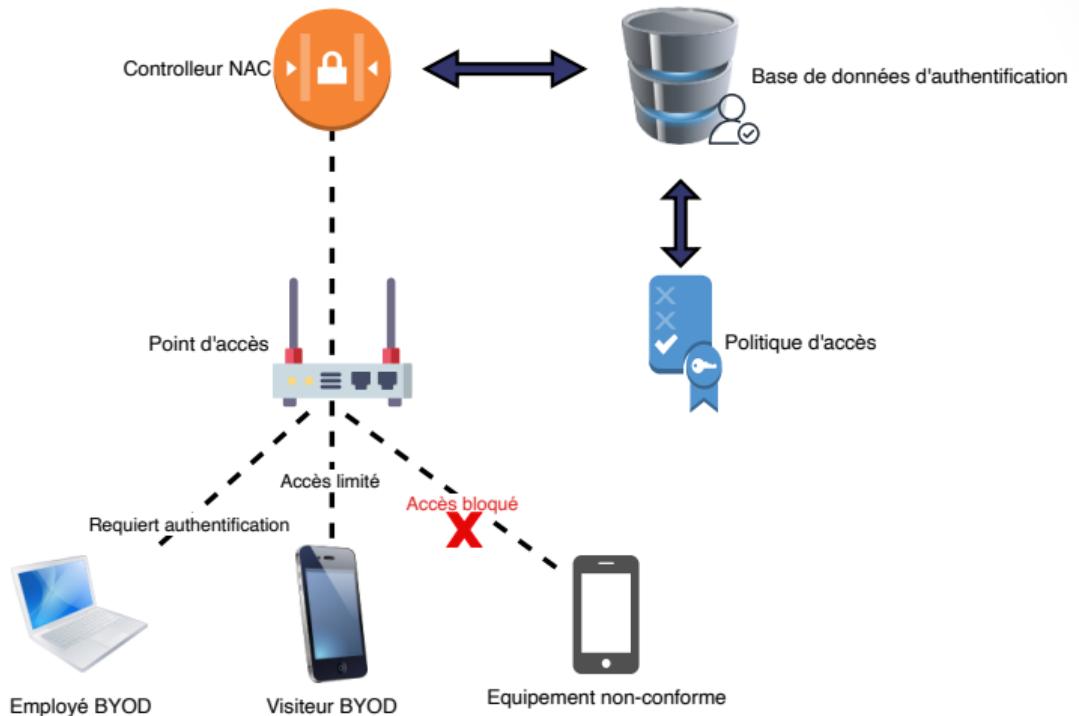


# IDS/IDP





## NAC : exemple utilisation contrôle BYOD





## NAC : Network Access Control

- # inspecte et assure que les équipements connectés ont une configuration et un état conforme avec la politique de sécurité
- # Le NAC peut vérifier qu'il y a un antivirus, un pare feu local
- # contrôle et limite les accès des BYOD, IOT et équipements des sous-traitants
- # met en quarantaine les pc infectés



## Opérations NAC 802.1X

**lancement** : l'authentificateur (par exemple un commutateur réseau) ou le demandeur (l'équipement client) envoie une requête de lancement de session. Un demandeur envoie un message de réponse EAP (TLS, token, etc.) à l'authentificateur, qui encapsule le message et le transmet au serveur d'authentification

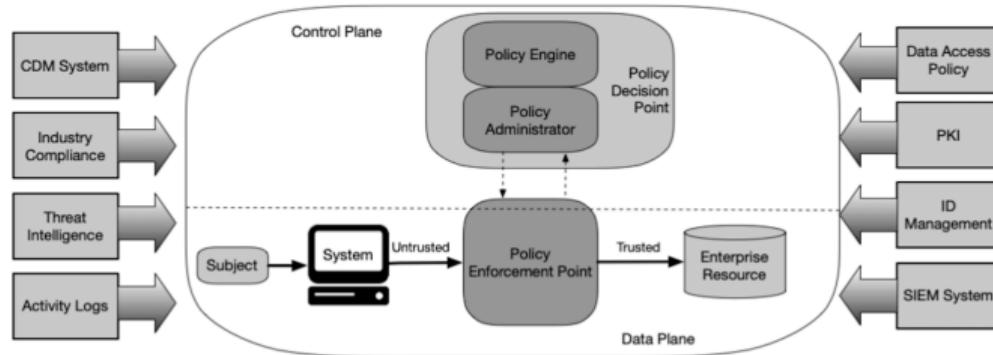
**authentification** : les messages transitent entre le serveur d'authentification et le demandeur via l'authentificateur pour valider plusieurs informations

**autorisation** : si les données d'identification sont valides, le serveur d'authentification informe l'authentificateur d'accorder l'accès au port au demandeur

**comptabilité** : le processus de comptabilité RADIUS enregistre les informations de session, notamment l'utilisateur, l'équipement, le type de session et le service

**clôture** : les sessions sont clôturées en déconnectant le point de terminaison ou en utilisant un logiciel de gestion

# ZTA NIST SP800-207



# Zero Trust



- # Limites du modèle de sécurité périmétrique : 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



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 que 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.

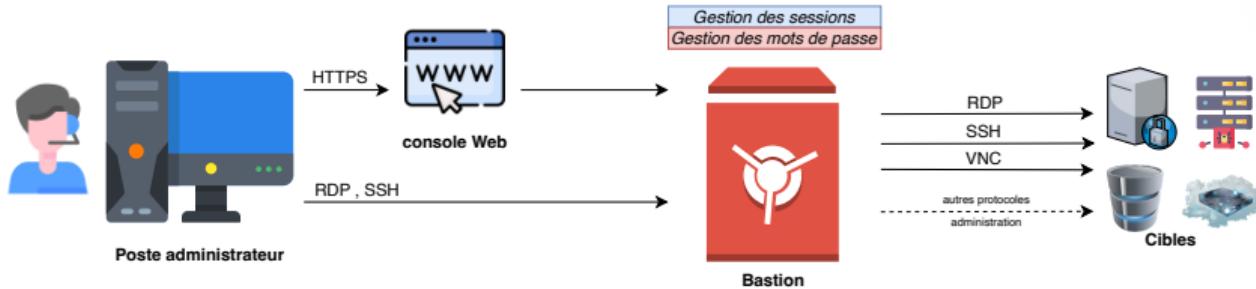
---

**ANSSI (AGENCE NATIONALE SÉCURITÉ DES SYSTÈMES D'INFORMATION)**

*RECOMMANDATIONS RELATIVES À L'ADMINISTRATION SÉCURISÉE DES SYSTÈMES D'INFORMATION v3-0*

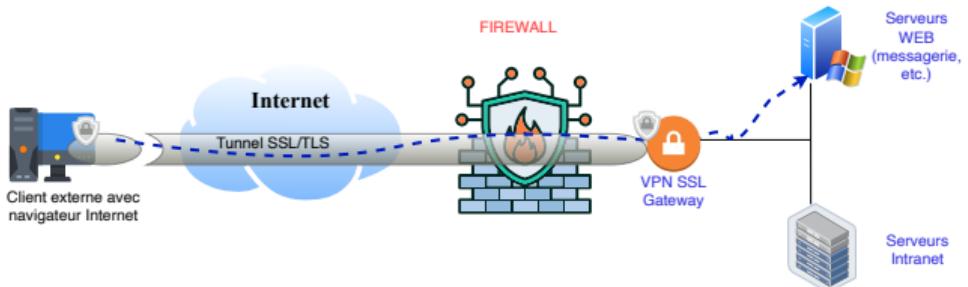
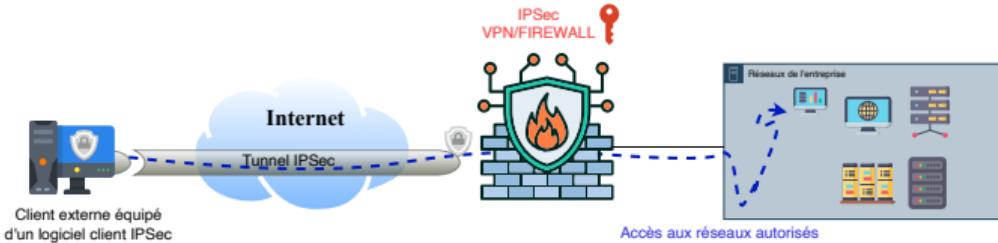


# Bastion





# VPN IPSec vs VPN SSL



# Cloud



Le Cloud, la réponse aux enjeux de résilience ?

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

# 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)

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

- # Le modèle du château fort demeure mais évolue
- # les technologies de protection et de 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



## 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-M3c-Architectures.przt.pdf sur GITHUB CYBERDEF ↗<sup>1</sup>](#)



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

