Orange CyberSchool

# Architectures, Composants et

Yann Arzel LE VILLIO, Orange CyberSchool

1er septembre 2023



#### **Abstract**

🗱 Hashtags : Architectures, composants sécurité, SSI

Ce document présente les architectures, Composants de cybersécurité.

Architectures, Composants et Sécurité

Yann Arzel LE VILLIO

1er septembre 2023

ntroduction architecture

De l'analyse de risques aux fonctions de sécurité

Architecture et composants de système d'information

Modèles de sécurité et technologies de écurité protectrices

écurité Endpoints

## Let's go

Architectures, Composants et Sécurité

Architectures, Composants et Sécurité

Yann Arzel I F VILLIO

1er septembre 2023

Introduction Architecture

De l'analyse de risques aux fonction de sécurité

Architecture et composants de système

Modèles de sécurité et technologies de sécurité protectrices

Sécurité Endpoints

#### **Sommaire**

- Introduction Architecture
- De l'analyse de risques aux fonctions de sécurité
  - Filtrage
  - Accès
  - Cryptographie
    - DéfinitionsConcepts
  - Architecture et composants de système
- d'information
- Middle
- Front
- Endpoints
- Réseau
   Modèles de sécurité et technologies de sécurité protectrices
  - Château fort (Firewall, Proxv. anti

- pare-feu
- Proxy et Reverse Proxy
- Sondes de détection (IDS/IDP)
- IAM , ZeroTrust, Bastion, VPN SSL, NAC
  - IAM
  - IAM
  - ZerotrustBastion
  - VPN SSL
  - Network Access Control : NAC CHAPITRE 5
  - plutot?
  - Cloud
    - MultiCloud Cloud Hybride
    - Cloud Access Security Broker CASBSecure access service edge (SASE)
- 5 Sécurité Endpoints
  - composants Endpoints
    - FW local

Composants et Sécurité

Architectures

1<sup>er</sup> septembre 2023

ntroduction

De l'analyse de isques aux fonctions

Architecture et composants de système

Modèles de sécurité et technologies de sécurité protectrices

counte Enapointe

4/2



- 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
- 5 Sécurité Endpoints

Architectures, Composants et Sécurité

Yann Arzel LE VILLIO

1er septembre 2023

#### Introduction Architecture

De l'analyse de risques aux fonction de sécurité

omposants de système

Modèles de sécurité et technologies de sécurité protectrices

écurité Endpoints

## Architectures, Composants et Sécurité

Introduction

- 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

Architectures, Composants et Sécurité

Yann Arzel I E VII I IO

1er septembre 2023

#### Introduction Architecture

De l'analyse de risques aux fonctions de sécurité

Architecture et composants de système

Modèles de sécurité et technologies de sécurité protectrices

Sécurité Endopints

- Introduction Architecture
- De l'analyse de risques aux fonctions de sécurité
  - Filtrage
  - Accès
  - Cryptographie

- 3 Architecture et composants de système d'information
- Modèles de sécurité et technologies de sécurité protectrices
- 5 Sécurité Endpoints

Architectures, Composants et Sécurité

Yann Arzel LE VILLIO

1er septembre 2023

ntroduction Architecture

De l'analyse de risques aux fonctions de sécurité

Filtrage

Accès

Cryptographie

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

exemples de traitement des risques

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

Architectures, Composants et Sécurité

Yann Arzel I F VILLIO

1er septembre 2023

ntroduction architecture

De l'analyse de risques aux fonctions de sécurité

Filtrage

Accès

Comtographi

Cryptographie

Architecture et composants de système

d'information

Modèles de sécurité et technologies de sécurité protectrices

Sécurité Endocints

Définitions et concepts

- Cryptologie : science du secret
- Algorithmes
  - Chiffrement à clefs secrètes
  - Cryptographie à clefs publiques
  - Fonction de hachage
  - Clefs

Architectures, Composants et Sécurité

Yann Arzel LE VILLIO

1er septembre 2023

Introduction Architecture

De l'analyse de risques aux fonctions de sécurité

Filtrag

Accès

Cryptographie

Architecture et composants de système

d'information

Modèles de sécurité et technologies de sécurité protectrices

Sécurité Endpoints

Clefs

- 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)

Architectures, Composants et Sécurité

Yann Arzel LE VILLIO

1er septembre 2023

Introduction Architecture

De l'analyse de risques aux fonctions de sécurité

Filtrage

Accès

On onto exemble

Architecture et composants de système

d'information

Modèles de sécurité et technologies de sécurité protectrices

Sécurité Endocints

De la confiance aux usages en entreprise

- 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.

Architectures Composants et Sécurité

Yann Arzel I F VII I IO

1er septembre 2023

Accès

De l'usure électronique au partage de confiance

- 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)

Architectures, Composants et Sécurité

Yann Arzel LE VILLIO

1er septembre 2023

Introduction Architecture

De l'analyse de risques aux fonctions de sécurité

Filtrage

Accès

Cryptograph

Cryptographie

Architecture et composants de système

Modèles de sécuri

et technologies de sécurité protectrices

Sécurité Endpoints

- 1 Introduction Architecture
- De l'analyse de risques aux fonctions de sécurité
- Architecture et composants de système d'information
  - Middle

- Front
- Endpoints
- Réseau
- Modèles de sécurité et technologies de sécurité protectrices
- 5 Sécurité Endpoints

Architectures, Composants et Sécurité

Yann Arzel LE VILLIO

1er septembre 2023

Introduction Architecture

De l'analyse de risques aux fonction de sécurité

Architecture et composants de système d'information

Middle

.

ndpoints

Enupoints

Modèles de sécurité et technologies de sécurité protectrices

Sécurité Endpoi

13/34



## Architecture et composants de système

#### d'information

exemples de traitement des risques

Front: Web, applications mobiles, clientless

2 Middle: BDD, Messagerie, ERP

Endpoints : PC, mobile, IoT

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

Architectures, Composants et Sécurité

Yann Arzel LE VILLIO

1er septembre 2023

troduction chitecture

De l'analyse de risques aux fonctions de sécurité

Architecture et composants de système

Middle

iviidale

Endpoints

Réseau

eseau

Modèles de sécurité et technologies de sécurité protectrices

Sécurité Endpoi

14/34

- Modèles de sécurité et technologies de sécurité protectrices

- Château fort (Firewall, Proxy, anti DDoS), cloisonnement, accès admin dédié
- Sondes de détection (IDS/IDP)
- IAM, ZeroTrust. Bastion, VPN SSL. NAC
  - Cloud

Architectures Composants et Sécurité

Yann Arzel I F VII I IO

1er septembre 2023

Modèles de sécurité et technologies de sécurité protectrices

IAM . ZeroTrust. Bastion.

#### Modèles de sécurité et technologies de

#### sécurité protectrices

Château fort

Architectures, Composants et Sécurité

Yann Arzel LE VILLIO

1er septembre 2023

ntroduction architecture

De l'analyse de

composan système d'informati

Modèles det technole

sécurité pr

oisonneme Imin dédié

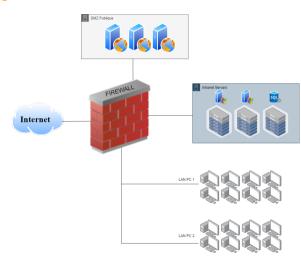
Château fort

pare-feu

des de détection

IAM , ZeroTrust, Bastion, VPN SSL, NAC

#### Château fort



#### Architectures, Composants et Sécurité

Yann Arzel LE VILLIO

1er septembre 2023

Introduction Architecture

De l'analyse de risques aux fonction de sécurité

Architecture et composants de système

Modèles de sécurité et technologies de sécurité protectrices

Château fort (Firewall, Proxy, anti DDoS), cloisonnement, accès admin dédié

#### Château fort

pare-feu

Proxy et Revers

Sondes de déte |DS/IDP)

IAM , ZeroTrust, Bastion, VPN SSL NAC

# Modèles de sécurité et technologies de sécurité protectrices

Firewall

- stateless (Access Control List : ACL)
- statefull
- Next generation

Architectures, Composants et Sécurité

Yann Arzel I F VILLIO

1er septembre 2023

ntroduction architecture

risques aux fonctio de sécurité

composants système d'informatio

> lodèles de sécu t technologies d

écurité prof Château fort (f

nateau fort (Fi roxy, anti DDo oisonnement,

Château fort

noro fou

pare-feu

Proxy et Reverse Pr

ndes de détection S/IDP)

IAM , ZeroTrust, Bastion, VPN SSL, NAC

## Modèles de sécurité et technologies de

#### sécurité protectrices

Proxv

Schéma Proxy

Architectures Composants et Sécurité

Yann Arzel I F VII I IO

1er septembre 2023

Proxy et Reverse Proxy

IAM . ZeroTrust. Bastion.

## Modèles de sécurité et technologies de

#### sécurité protectrices

**Reverse Proxy** 

Schéma Reverse Proxy

Architectures Composants et Sécurité

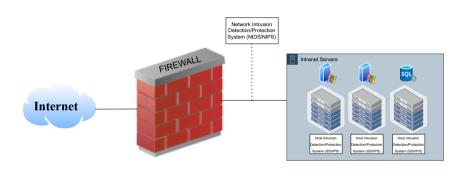
Yann Arzel I F VII I IO

1er septembre 2023

Proxy et Reverse Proxy

IAM . ZeroTrust. Bastion.

#### **IDS/IDP**



Architectures, Composants et Sécurité

Yann Arzel LE VILLIO

1er septembre 2023

ntroduction Architecture

De l'analyse de risques aux fonctions de sécurité

Architecture et composants de système

Modèles de sécurité et technologies de sécurité protectrices

Château fort (Firewall, Proxy, anti DDoS), cloisonnement, accès admin dédié

#### Sondes de détection (IDS/IDP)

IAM , ZeroTrust, Bastion, VPN SSL, NAC

Cloud

écurité Endpo

# Modèles de sécurité et technologies de sécurité protectrices

sondes de détection (IDS/IDP)

Schéma sondes de détection (IDS/IDP)

Architectures, Composants et Sécurité

Yann Arzel I F VILLIO

1er septembre 2023

troduction rchitecture

De l'analyse de risques aux fonctions

Architecture et composants de système

Modèles de sécurité

technologies de curité protectrices

aâteau fort (Firewall, oxy, anti DDoS), oisonnement, accès

#### Sondes de détection (IDS/IDP)

IAM , ZeroTrust, Bastion, VPN SSL, NAC

Cloud

nto Enapointo

#### Gestion des identités : IAM

**Identity Access Management** 

- Définition
  - IAM (identity and access management)
  - IAG (identity access governance)
  - DAG (data access governance)
  - PAM (privileged access management)
- Process Gestion des identités cycle de vie
- Procédures Contrôle des habilitations

Architectures, Composants et Sécurité

Yann Arzel LE VILLIO

1er septembre 2023

Introduction Architecture

De l'analyse de risques aux fonctions de sécurité

Architecture et composants de système

Modèles de sécurité et technologies de sécurité protectrices

Château fort (Firewall, Proxy, anti DDoS), cloisonnement, accès admin dédié

Sondes de détect (IDS/IDP)

IAM , ZeroTrust, Bastion, VPN SSL, NAC

IAM

Zerotrust

tion

#### **Zerotrust**

- 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

Architectures, Composants et Sécurité

Yann Arzel LE VILLIO

1er septembre 2023

Introduction Architecture

De l'analyse de risques aux fonctior de sécurité

Architecture et composants de système

Modèles de sécurité et technologies de sécurité protectrices

Château fort (Firewall, Proxy, anti DDoS), cloisonnement, accès admin dédié

Sondes de déte (IDS/IDP)

IAM , ZeroTrust, Bastion, VPN SSL, NAC

AM

Zerotrust

Bastion

#### **Bastion**

#### Architectures, Composants et Sécurité

Yann Arzel I F VII LIO

1er septembre 2023

Bastion

schéma

#### **VPN SSL**

Architectures, Composants et Sécurité

Yann Arzel LE VILLIO

1er septembre 2023

ntroduction architecture

e l'analyse de sques aux fon e sécurité

hitecture et

informatio

odèles de technolo

ateau fort (

y, anti DD onnement in dédié

3/IDP) 1 , ZeroT

n SSL, n M

M

erotrust

on

schéma

#### **NAC**

- 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 Schéma?

Architectures, Composants et Sécurité

Yann Arzel LE VILLIO

1er septembre 2023

Architecture

risques aux fonctior de sécurité

Architecture et composants de système

Modèles de sécurité et technologies de sécurité protectrices

Château fort (Firewall, Proxy, anti DDoS), cloisonnement, accès admin dédié

Sondes de détect (IDS/IDP)

IAM , ZeroTrust, Bastion, VPN SSL, NAC

AM.

\_\_\_\_\_\_

Bastion

#### 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;
- NGFW (firewalls de nouvelle génération);
- zero trust network access (ZTNA).

Architectures, Composants et Sécurité

Yann Arzel LE VILLIO

1er septembre 2023

ntroduction architecture

De l'analyse de risques aux fonction

Architecture et composants de système

Modèles de sécurité et technologies de

et technologies de sécurité protectrices

Château fort (Firewall, Proxy, anti DDoS), cloisonnement, accès

Sondes de détection

IAM , ZeroTrust, Bas

loud

Cloud - Cloud ide

#### Cloud

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

Architectures, Composants et Sécurité

Yann Arzel LE VILLIO

1er septembre 2023

Architecture

De l'analyse de risques aux fonctions de sécurité

Architecture et composants de système

Modèles de sécurité et technologies de

Château fort (Firewall, Proxy, anti DDoS),

dmin dédié iondes de détection

(IDS/IDP)

Cloud

Cloud - Cloud ide

#### **Cloud Access Security Broker - CASB**

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

Architectures, Composants et Sécurité

Yann Arzel LE VILLIO

1er septembre 2023

Architecture

De l'analyse de risques aux fonctions de sécurité

Architecture et composants de système

Modèles de sécurité

ècurité protectrices Château fort (Firewall, Proxy, anti DDoS),

loisonnement, accès dmin dédié

Sondes de détection (IDS/IDP)

VPN SSL, NAC

Cloud

ide

- Introduction Architecture
- De l'analyse de risques aux fonctions de sécurité
- 3 Architecture et composants de système d'information

- Modèles de sécurité et technologies de sécurité protectrices
- Sécurité Endpoints
  - composants Endpoints
  - FW local
  - Antivirus
  - EDS/EDR
  - Exemple

Architectures, Composants et Sécurité

Yann Arzel LE VILLIO

1er septembre 2023

ntroduction 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

omposants Endpo

....

Antivirus

.....

21/2/

## Des questions!

Eric Dupuis



#### **Contributions**

GitHub

Les notes et les présentations sont réalisées sous LETEX. 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 évogués.

Les fichiers sources sont publiés sur GITHUB dans l'espace : (edufaction/CYBERDEF101) 🚰 a.

Architectures, Composants et Sécurité

Yann Arzel I F VII LIO

1er septembre 2023

troduction rchitecture

De l'analyse de risques aux fonctions de sécurité

Architecture et composants de système

Modèles de sécurité et technologies de sécurité protectrices

Sécurité Endpoints

omposants Endpoi

. .. .

Antivirus

.

Exemple

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

## Mises à jour régulières

Eduf@ction yann-arzel.levillio@orange.com

Vérifiez la disponibilité d'une version plus récente de



2023 eduf@ction - Publication en Creative Common BY-NC-ND



Architectures, Composants et Sécurité

Yann Arzel I F VILLIO

1er septembre 2023

troduction rchitecture

De l'analyse de risques aux fonctions de sécurité

Architecture et composants de système

Modèles de sécurité et technologies de sécurité protectrices

Sécurité Endpoints

mposants Endpoi

1 11 1000

Antivirus

\_ .

Exemple

34/34

