BStorm

DEVOPS SÉCURISATION

PRÉREQUIS

- **Linux :** Aisance avec le terminal (bash).
- **Admin Sys :** Gestion des paquets, services, utilisateurs.
- **Réseau :** Notions IP, Ports, SSH.

OBJECTIFS PÉDAGOGIQUES

FONDAMENTAUX

Maîtriser CIA & Defense in Depth.

ACCÈS

Sécuriser SSH & implémenter RBAC.

CRYPTO

Gérer PKI & Certificats SSL.

DEVSECOPS

Sécurité dans le pipeline.

PROGRAMME DE LA JOURNÉE

1. Principes Fondamentaux
2. Authentification & Autorisation
3. Chiffrement & Certificats

1. Hardening Système
2. Sécurité Réseau
3. DevSecOps & Pipeline

ENVIRONNEMENT DE LAB

```
VMs Linux (Ubuntu 20.04/22.04 LTS)
Accès ROOT obligatoire (sudo)
Environnement isolé (Sandbox)
```

⚠️ Attention : Les techniques démontrées peuvent être destructrices.

01

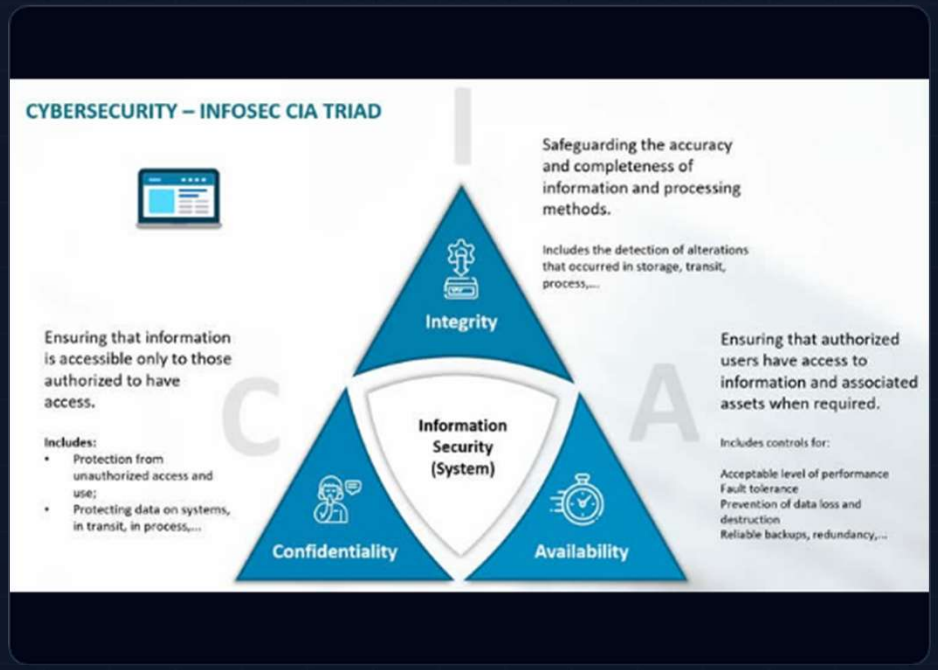
PRINCIPES FONDAMENTAUX

LA TRIADE CIA

LE MODÈLE DE RÉFÉRENCE

Tout incident de sécurité impacte au moins un de ces trois piliers.

- **Confidentialité**
- **Intégrité**
- **Disponibilité**



CONFIDENTIALITÉ

Définition : L'information n'est accessible qu'aux personnes autorisées.

MENACES	CONTRÔLES
Sniffing, Vol de données, Social Engineering	Chiffrement (AES), ACLs, MFA

INTÉGRITÉ

Définition : L'information est fiable et n'a pas été altérée.

```
$ sha256sum backup.tar.gz
e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855
```

Utilisation de signatures numériques et de checksums.

DISPONIBILITÉ

Définition : Les systèmes fonctionnent quand on en a besoin.

ATTAQUES

DDoS, Ransomware, Sabotage physique.

DÉFENSES

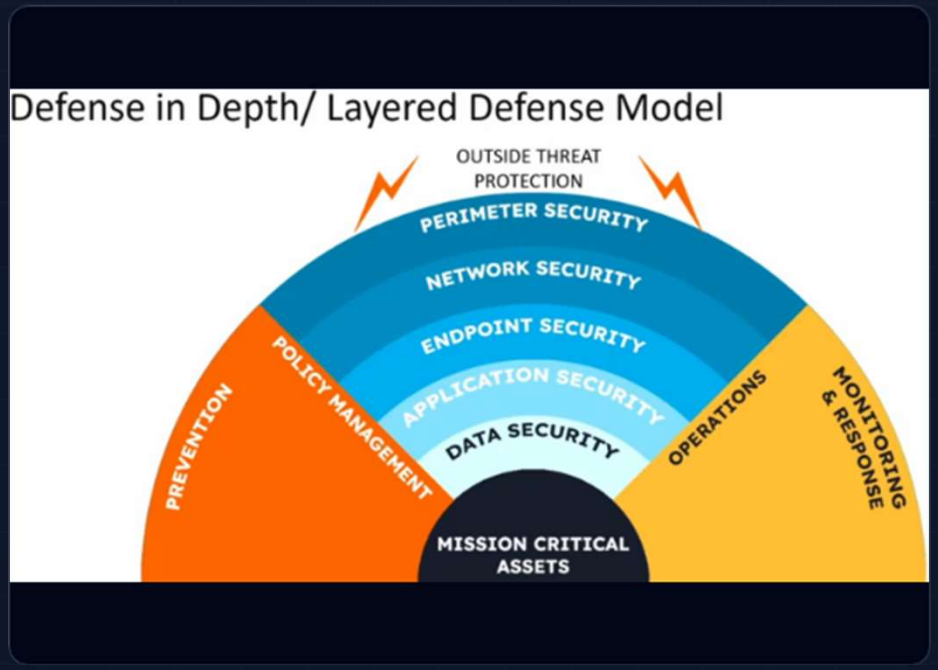
Redondance, Backups, Load Balancing.

DEFENSE IN DEPTH (DÉFENSE EN PROFONDEUR)

L'APPROCHE "OIGNON"

Ne jamais compter sur une seule barrière. Superposer les couches de sécurité.

Périmètre > Réseau > Hôte > App > Data



PRINCIPE DU MOINDRE PRIVILÈGE (POLP)

> "Accès Minimum Nécessaire"

- Un utilisateur ne doit pas être admin par défaut.
- Un service web ne doit pas tourner en root.
- Une clé API ne doit avoir accès qu'à son scope.

LA SURFACE D'ATTAQUE

CONCEPT

La somme de tous les vecteurs potentiels qu'un attaquant peut utiliser.

Objectif : Réduire la surface.

Fermer les ports inutiles
Désinstaller les logiciels superflus

SECURITY BY DESIGN

Intégrer la sécurité dès la conception, pas comme une "cerise sur le gâteau" à la fin du projet.

PROACTIF

Prévenir plutôt que guérir

PAR DÉFAUT

Configuration sécurisée out-of-the-box

SYNTHÈSE SECTION 1

- CIA est notre boussole.
- Multiplier les couches de défense.
- Toujours appliquer le moindre privilège.

02

AUTHENTIFICATION & AUTORISATION

AUTHN VS AUTHZ

AUTHENTIFICATION

Qui êtes-vous ?
(Login, Clés)

AUTORISATION

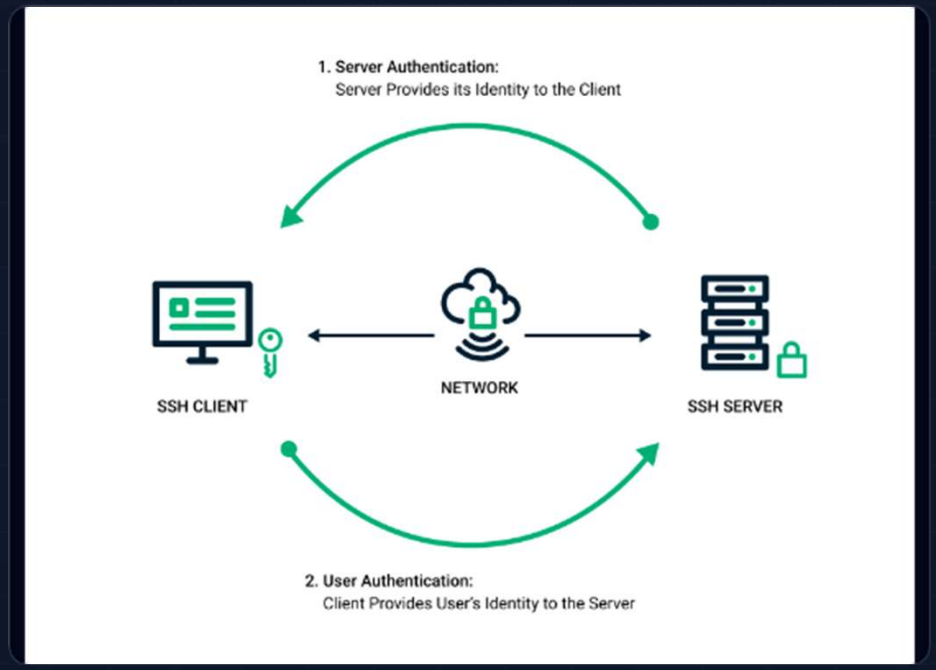
Que pouvez-vous faire ?
(Permissions, Sudo)

SSH : SECURE SHELL

LE STANDARD DE FACTO

Remplace Telnet. Communication chiffrée.

Authentification par mot de passe (déconseillé) ou par clés (recommandé).



GÉNÉRER UNE PAIRE DE CLÉS SSH

```
$ ssh-keygen -t ed25519 -C "admin@server"
Generating public/private ed25519 key pair.
Your identification has been saved in /home/user/.ssh/id_ed25519
Your public key has been saved in /home/user/.ssh/id_ed25519.pub
```

ED25519 est plus rapide et sûr que RSA.

PUBLIC VS PRIVATE KEY

PRIVÉE

Gardée secrète sur votre PC.
NE JAMAIS PARTAGER.

PUBLIQUE

Copiée sur les serveurs.
Peut être partagée.

DÉPLOYER LA CLÉ

Utilitaire pour copier la clé publique vers `~/.ssh/authorized_keys` :

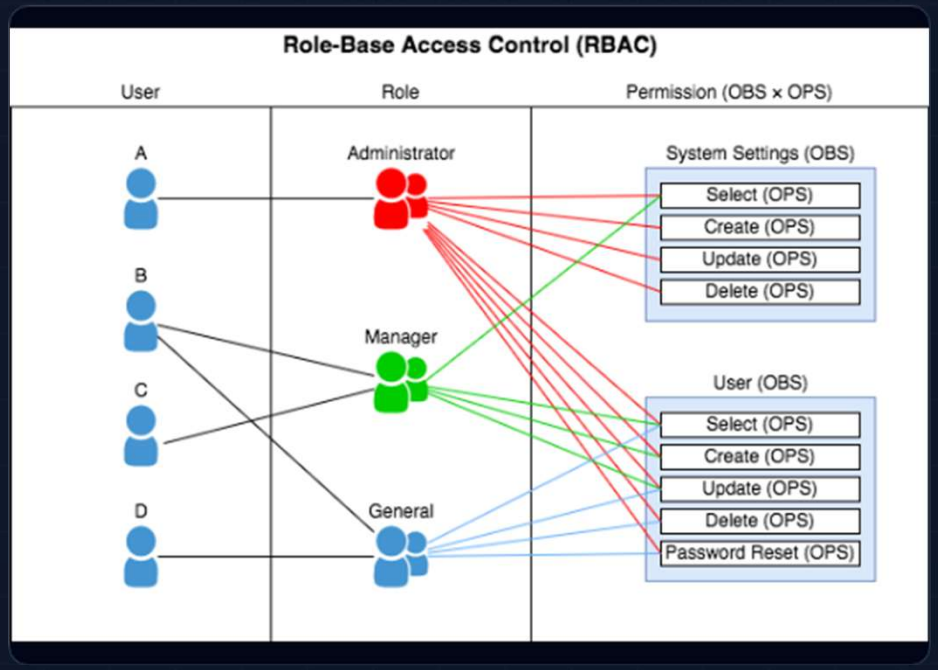
```
$ ssh-copy-id user@192.168.1.50
```

Ensuite, désactiver l'authentification par mot de passe dans `/etc/ssh/sshd_config`.

RBAC (ROLE BASED ACCESS CONTROL)

GESTION DES DROITS

On n'assigne pas de droits aux utilisateurs, mais à des Rôles. Les utilisateurs reçoivent des rôles.



SUDOERS

Configuration dans `/etc/sudoers` (utiliser `visudo`).

```
# User privilege specification
root ALL=(ALL:ALL) ALL

# Allow members of group sudo to execute any command
%sudo ALL=(ALL:ALL) ALL
```

MFA (MULTI-FACTOR AUTHENTICATION)

CE QUE JE SAIS	CE QUE J'AI	CE QUE JE SUIS
Mot de passe	Token (YubiKey, TOTP)	Biométrie

PAM (PLUGGABLE AUTHENTICATION MODULES)

Framework Linux pour gérer l'authentification.

Permet d'ajouter Google Authenticator à SSH.

```
$ sudo apt install libpam-google-authenticator
```

GESTION DES MOTS DE PASSE

- Longueur > Complexité.
- Ne jamais réutiliser.
- Utiliser un gestionnaire de mots de passe (Bitwarden, Keepass).
- Rotation forcée = Mauvaise pratique (encourage les mots de passe faibles).

LAB : SÉCURISATION SSH

1. Créer une clé SSH.
2. La copier sur la VM.
3. Désactiver PasswordAuthentication.
4. Désactiver PermitRootLogin.

03

CHIFFREMENT & CERTIFICATS

POURQUOI CHIFFRER ?

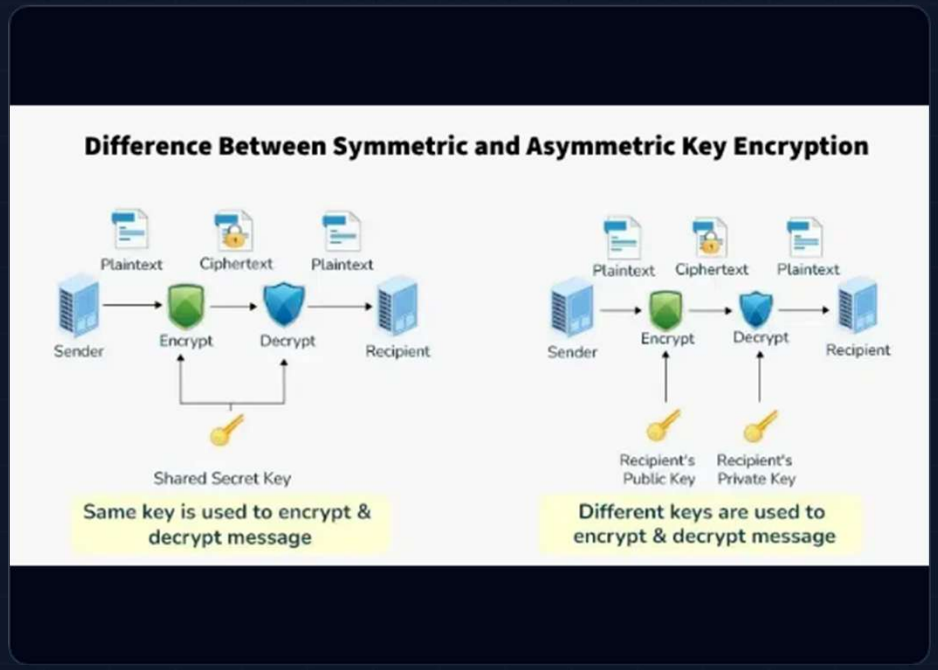
- Protéger la confidentialité (Data at Rest).
- Protéger le transport (Data in Transit).
- Garantir l'authenticité.

SYMÉTRIQUE VS ASYMÉTRIQUE

LA DIFFÉRENCE CLÉ

Symétrique : Une seule clé (Rapide).
Ex: AES.

Asymétrique : Paire de clés (Lent, échange sécurisé).
Ex: RSA, ECC.



FONCTION DE HACHAGE

Empreinte numérique unique (One-way).

Si un bit change dans le fichier, le hash change complètement.

```
MD5 (Obsolète, collisions)
SHA-1 (Obsolète)
SHA-256 (Standard actuel)
```

PKI (PUBLIC KEY INFRASTRUCTURE)

LA CHAÎNE DE CONFIANCE

Comment faire confiance à une clé publique ? Elle est signée par une entité de confiance (CA).

CA Racine > CA Intermédiaire > Certificat Final

CERTIFICATS X.509

Carte d'identité numérique du serveur.

- **Subject :** Qui je suis (CN=google.com).
- **Issuer :** Qui me valide (Let's Encrypt).
- **Validity :** Date d'expiration.
- **Public Key :** Ma clé.

SSL VS TLS

SSL (SECURE SOCKETS LAYER)

Obsolète et vulnérable (POODLE, Heartbleed).

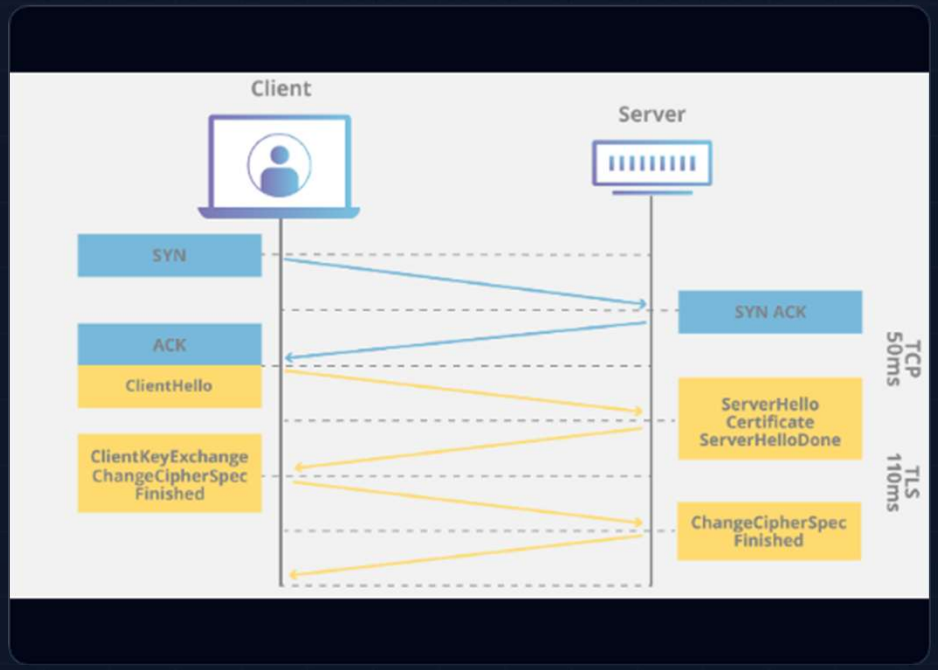
TLS (TRANSPORT LAYER SECURITY)

Le standard actuel. TLS 1.2 et 1.3 sont recommandés.

TLS HANDSHAKE

LA POIGNÉE DE MAIN

1. Négociation des algorithmes.
2. Échange de certificats.
3. Création de la clé de session (symétrique) via asymétrique.



OPENSSL : LE COUTEAU SUISSE

Outil ligne de commande pour tout faire en crypto.

- Générer des clés
- Créer des CSR
- Déboguer TLS

OPENSSL : COMMANDES UTILES

```
# Voir un certificat
openssl x509 -in cert.pem -text -noout

# Tester une connexion
openssl s_client -connect google.com:443
```

LET'S ENCRYPT & CERTBOT

CA gratuite et automatisée.

```
$ sudo apt install certbot python3-certbot-nginx
$ sudo certbot --nginx
```

Renouvellement automatique tous les 90 jours.

LAB : CRÉER UN CERTIFICAT AUTO-SIGNÉ

```
openssl req -x509 -newkey rsa:4096 \
-keyout key.pem -out cert.pem \
-days 365 -nodes
```

Utile pour le dev/test, mais lève une alerte dans le navigateur.

04

HARDENING SYSTÈME

POURQUOI DURCIR ?

Une installation par défaut est conçue pour l'utilisabilité, pas la sécurité.

Le Hardening consiste à verrouiller le système pour réduire sa surface d'attaque.

SERVICES INUTILES

Si vous ne l'utilisez pas, éteignez-le.

```
$ systemctl list-unit-files --state=enabled
$ systemctl disable cups
$ systemctl stop avahi-daemon
```

MISES À JOUR (PATCH MANAGEMENT)

CRITIQUE

Les failles (CVE) sont découvertes chaque jour. Un système non patché est vulnérable en quelques heures.

AUTOMATISER

`unattended-upgrades` sur Debian/Ubuntu pour les patches de sécurité.

PERMISSIONS DE FICHIERS

Comprendre `rwx` (Read, Write, Execute).

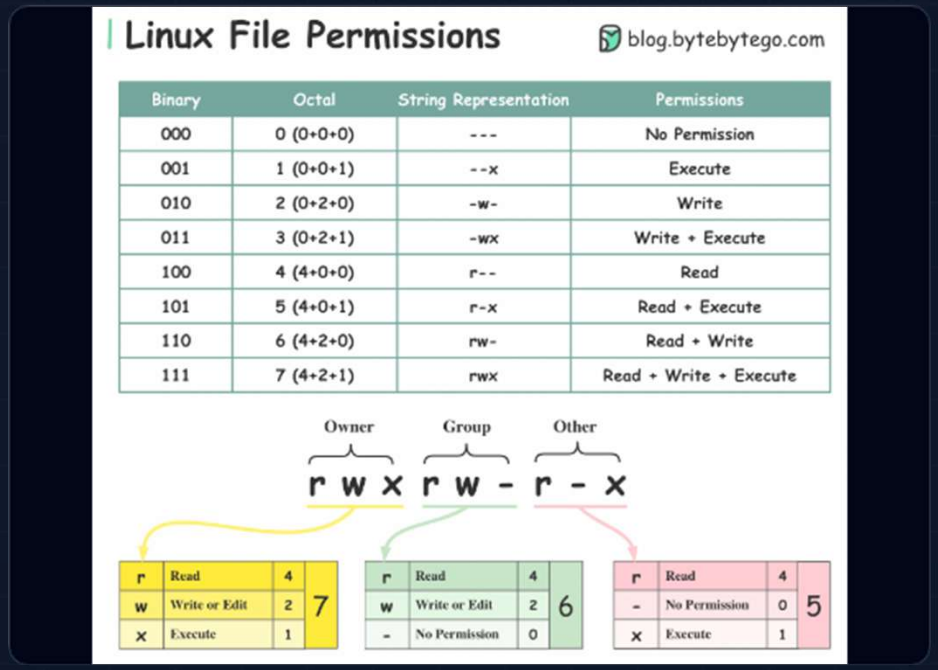
```
chmod 777 file # DANGER (Tout le monde peut tout faire)
chmod 600 key.pem # BON (Seul le propriétaire lit/écrit)
chmod 755 script.sh # BON (Exécutable par tous, modifiable par owner)
```

VISUALISER LES PERMISSIONS

STRUCTURE

User / Group / Others.

Le bit `setuid` peut être dangereux s'il est mal utilisé.



KERNEL HARDENING (SYSCTL)

Modifier les paramètres du noyau dans `/etc/sysctl.conf`.

```
# Désactiver ICMP Redirects
net.ipv4.conf.all.accept_redirects = 0
# Ignorer ICMP Broadcast
net.ipv4.icmp_echo_ignore_broadcasts = 1
```

AUDIT & LOGS

SAVOIR CE QUI SE PASSE

Les logs sont la boîte noire de votre serveur.

- `/var/log/auth.log` (Auth)
- `/var/log/syslog` (Général)

CENTRALISATION

Envoyer les logs vers un serveur externe (ELK, Splunk) pour éviter qu'ils soient effacés par l'attaquant.

OUTILS D'AUDIT

LYNIS

Scanner de sécurité local.

AUDITD

Surveillance des appels système.

AIDE

Détection d'intrusion fichiers.

SÉCURITÉ DU BOOTLOADER

Protéger GRUB avec un mot de passe pour empêcher la modification des paramètres de démarrage (ex: `init=/bin/bash` pour devenir root sans mot de passe).

CHIFFREMENT DE DISQUE (LUKS)

Si un attaquant vole physiquement le disque dur, les données doivent être illisibles.

Essentiel pour les laptops et serveurs physiques.

LAB : HARDENING AVEC LYNIS

```
$ sudo apt install lynis
$ sudo lynis audit system
```

Analyser le rapport et corriger 3 vulnérabilités détectées.

05

SÉCURITÉ RÉSEAU

PARE-FEU (FIREWALL)

LE PORTIER

Filtre le trafic entrant et sortant.

Politique par défaut : Tout bloquer (DROP), n'autoriser que le nécessaire.

Ports communs:
22 (SSH), 80/443 (Web)

UFW (UNCOMPLICATED FIREWALL)

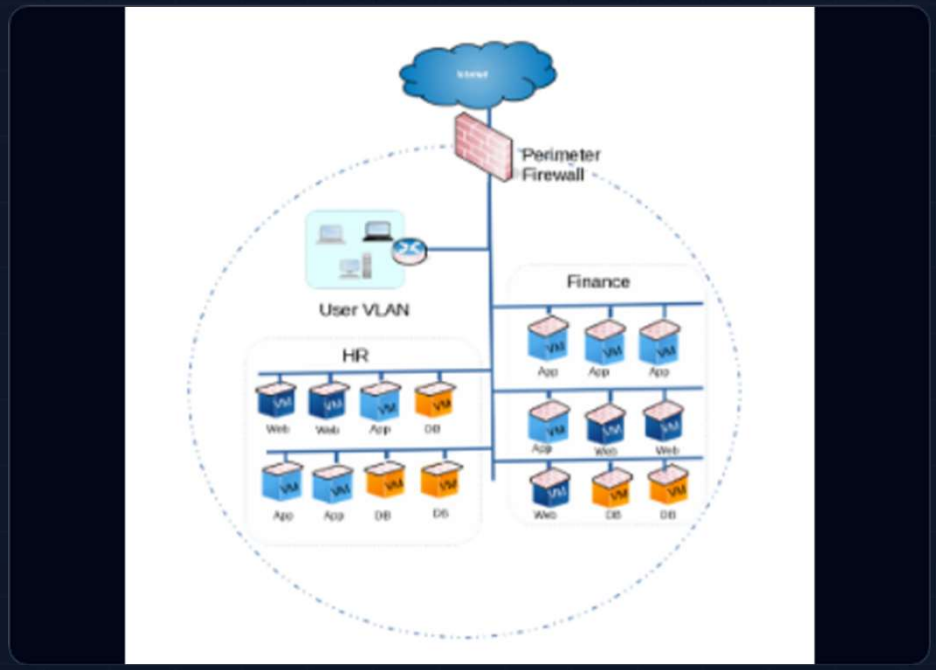
Interface simplifiée pour iptables.

```
$ ufw default deny incoming
$ ufw allow ssh
$ ufw allow 80/tcp
$ ufw enable
```

SEGMENTATION RÉSEAU

ISOLER LES SERVICES

Empêcher le mouvement latéral. Si le serveur web est compromis, la base de données reste protégée dans un autre VLAN.



FAIL2BAN

IPS (Intrusion Prevention System) léger.

Bannit dynamiquement les IPs qui échouent trop de tentatives de connexion.

```
[sshd]
enabled = true
maxretry = 3
bantime = 1h
```

VPN (VIRTUAL PRIVATE NETWORK)

Ne jamais exposer les services d'administration (SSH, Database, Dashboards) directement sur Internet.

Utiliser un VPN (WireGuard, OpenVPN) pour accéder au réseau interne.

NMAP : SCANNER DE PORTS

Outil pour auditer votre propre réseau et voir ce qui est exposé.

```
$ nmap -sV -p- 192.168.1.50
```

DMZ (ZONE DÉMILITARISÉE)

Zone tampon exposée à Internet.

Contient les serveurs publics (Web, Mail).

Ne peut pas initier de connexions vers le réseau interne sécurisé.

TCP WRAPPERS

Couche de sécurité supplémentaire pour certains services (`/etc/hosts.allow`, `/etc/hosts.deny`).

Moins utilisé aujourd'hui au profit des pare-feux, mais utile pour la défense en profondeur.

LAB : CONFIGURER UFW & FAIL2BAN

1. Autoriser SSH.
2. Activer UFW.
3. Installer Fail2Ban.
4. Tenter 5 échecs SSH et vérifier le ban.

06

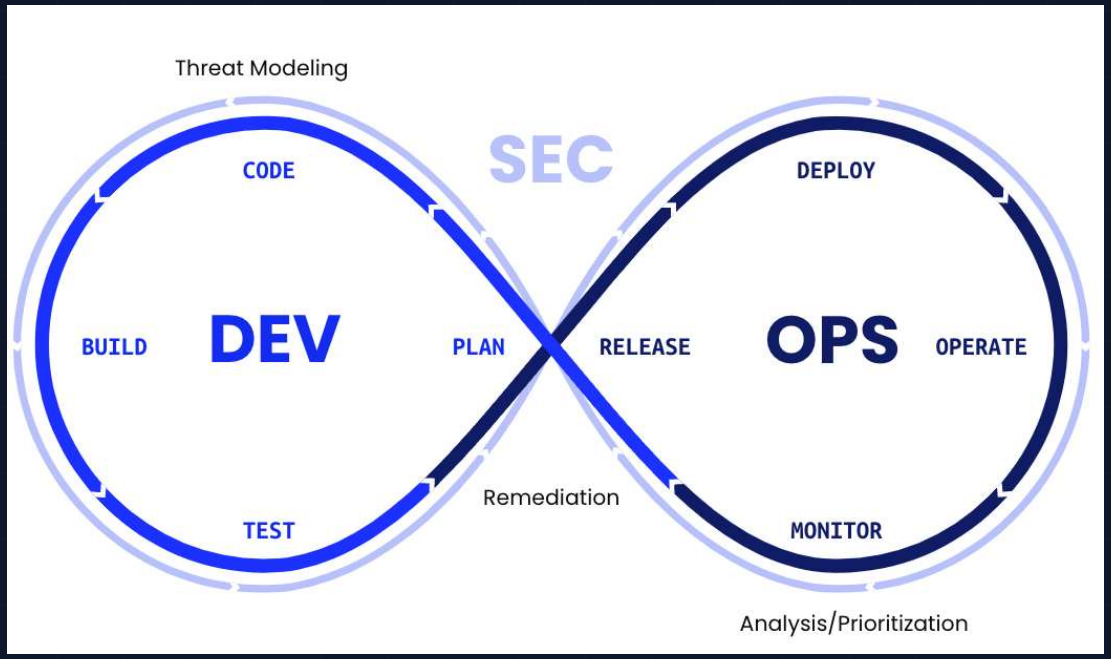
DEVSECOPS

LE PIPELINE DEVSECOPS

SHIFT LEFT

Intégrer la sécurité tôt dans le cycle, pas à la fin.

Code > Build > Test > Deploy > Monitor



SAST & DAST

SAST (STATIC)

Analyse du code source.
White Box.
Ex: SonarQube.

DAST (DYNAMIC)

Scan de l'app en exécution.
Black Box.
Ex: OWASP ZAP.

SCA (SOFTWARE COMPOSITION ANALYSIS)

Vos dépendances (NPM, Maven, Pip) sont-elles vulnérables ?

Outils : OWASP Dependency Check, Snyk, Dependabot.

```
> Found CVE-2023-1234 in lodash v4.17.15
> Critical Severity
```

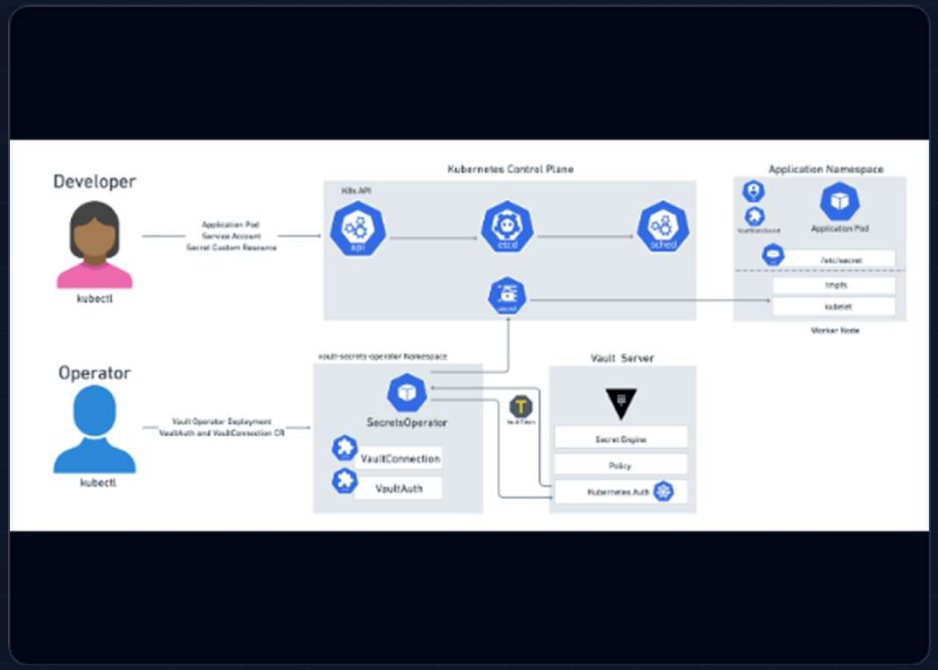
SECRETS MANAGEMENT

LE PROBLÈME

Secrets hardcodés dans Git.

LA SOLUTION

Vault, AWS Secrets Manager.



CONTAINER SECURITY

- Scanner les images Docker (Trivy, Clair).
- Ne pas utiliser `root` dans le conteneur.
- Utiliser des images de base minimales (Alpine, Distroless).

```
$ trivy image my-app:latest
```

INFRASTRUCTURE AS CODE (IAC)

Scanner les fichiers Terraform/Ansible pour des mauvaises configurations (ex: S3 bucket public).

Outils : tfsec, Checkov.

RÉCAPITULATIF

1. PRINCIPES

CIA, DiD

2. ACCÈS

SSH, MFA

3. HARDENING

Patch, FW

4. PIPELINE

Scan auto

IMAGE SOURCES

https://miro.medium.com/0*ZE2dgfCfy4tU4GpJ.jpg

Source: medium.com

https://miro.medium.com/1*wYUTKw8NHxvlZ1YZ6o1NNA.png

Source: aws.plainenglish.io

https://www.sectigo.com/uploads/images/SSH-Authentication.png

Source: www.sectigo.com

https://miro.medium.com/1*ub3g0nUC6NCkYPHoNB6rFw.png

Source: dsonoda.medium.com

https://media.geeksforgeeks.org/wp-content/uploads/20250203184531397403/symmetric-and-asymmetric-key-1-2.webp

Source: www.geeksforgeeks.org

https://cf-assets.www.cloudflare.com/slt3lc6tev37/5aYOr5erfyNBq20X5djTco/3c859532c91f25d961b2884bf521c1eb/tls-ssl-handshake.png

Source: www.cloudflare.com

IMAGE SOURCES

https://assets.bytebytego.com/diagrams/0259-linux-permissions-copy.png

Source: bytebytego.com

https://nilesecure.com/wp-content/uploads/2024/09/network-segmentation-1.png

Source: nilesecure.com

https://www.hackerone.com/sites/default/files/inline-images/DevSecOps%20Pipeline.png

Source: www.hackerone.com

https://www.datocms-assets.com/2885/1691011664-k8s-vault-sidecar-workflow-copy-2x.png

Source: www.hashicorp.com