Qualité et sécurité d’un service de chiffrement

Speakers

Jessim Nekkaa

Developer

nekkaajessim@yahoo.fr

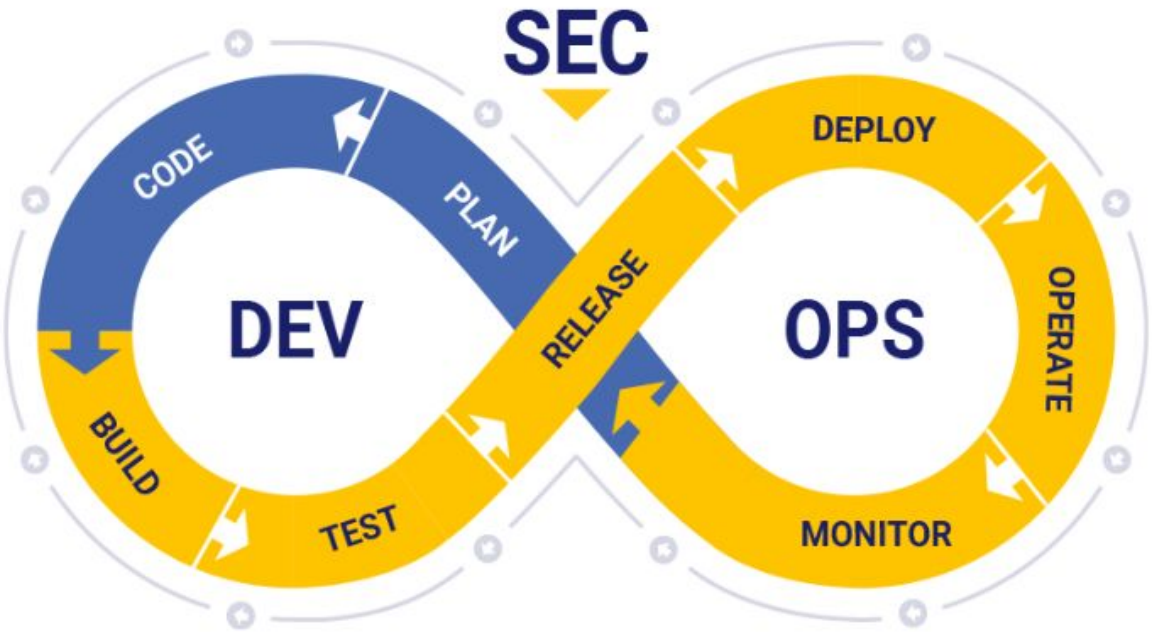
Johan Girard

Technical Leader

johan.girard@stormshield.eu

Développement Sécurisé

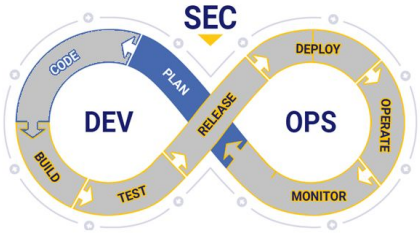
Développement sécurisé



Développement sécurisé

Plan

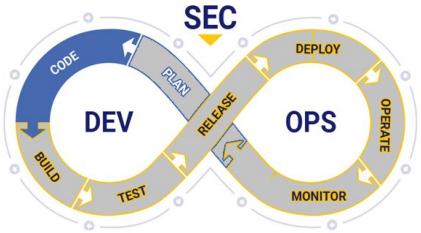
- Secured by Design
  - OWASP SAMM – Software Assurance Maturity Model
  - BSIMM – Building Security in Maturity Model
- Risk analysis
  - Key / Secret Life Cycle
- SDLC - Software Development Life Cycle
- Secure Development Guidelines
  - OWASP Guidelines
  - Guide ANSSI - Règles de programmation sécurisé



Développement sécurisé

Code

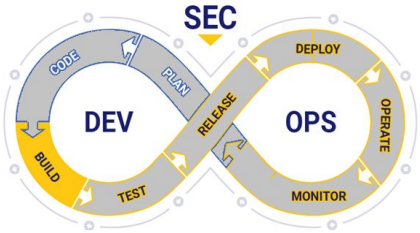
- Guidelines
  - Input validation, sanitization
  - Errors, logs
  - Cryptographic practices
  - Coding practices, architecture
  - Memory managements
- Secret Management
  - pipeline, dynamic, automatic rotation
- Vulnerability scanners
  - CVE, misconfigurations
- Linter



Développement sécurisé

Build

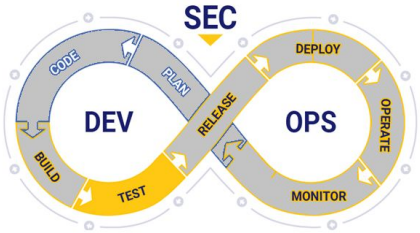
- Automated build process
    - CICD, IaC …
- SAST – Static Application Security Testing
- SCA – Software Composition Analysis
- Secure images
    - Vuln scan
    - Official images
    - Non-root, remove privileges, SELinux …



Développement sécurisé

Test

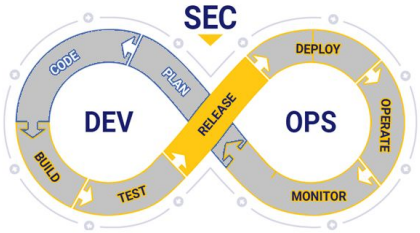
- DAST – Dynamic Application Security Testing
- Pen Test
- Fuzzing Test
- Non-functional testing (scalability, reliability…)



Développement sécurisé

Release

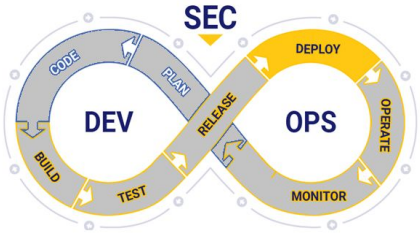
- Sign software
- SBOM – Software Bill of Materials
- Vulnerability Management → Monitoring



Développement sécurisé

Deploy

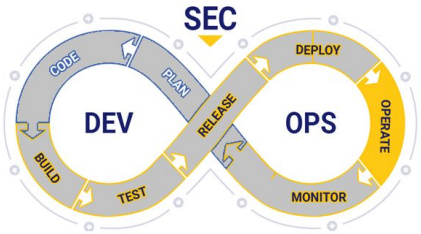
- Hardening
  - AppArmor
  - Seccomp
- Secrets Management
- Kubernetes Security
  - Kubernetes Role-Based Access Control
  - Firewall in/out
  - SSL between components



Développement sécurisé

Operate

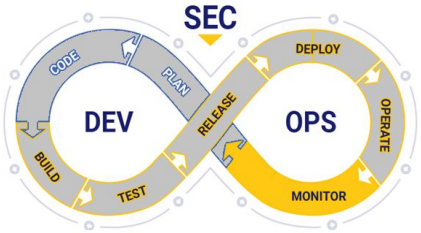
- RASP – Runtime Application Self-Protection
    - Falco
- WAF – Web Application Firewall
- Anti-DDoS
- Chaos Testing
- IAM – Identity and Access Management
- EDR – Endpoint Detection and Response



Développement sécurisé

Monitor

- Security Audit
- SIEM – Security Information and Event Management
- SOC – Security Operations Centers
- CNAPP – Cloud Native Application Protection
    - CSPM – Cloud Security Posture Management
    - CIEM – Cloud Infrastructure Entitlement Management
    - CWPP – Cloud Workload Protection Platform



Chiffrement
à l'échelle industrielle

Chiffrement à l'échelle industrielle

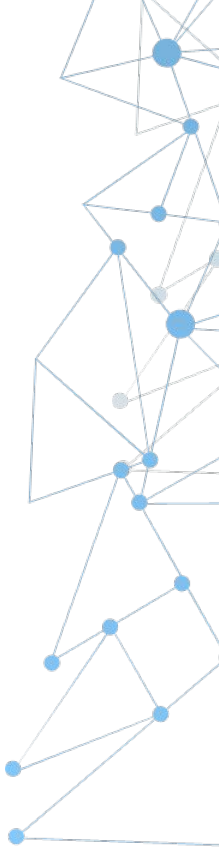
Définition

- Chiffrement de gros volume de données
- Sécuriser des systèmes et infrastructures

=> Sécurité, confidentialité et intégrité des informations

Problématiques

- Comment chiffrés beaucoup de données ?
- Comment gérer nos clés de chiffrement ?
- Ou effectuer les opérations cryptographique ?

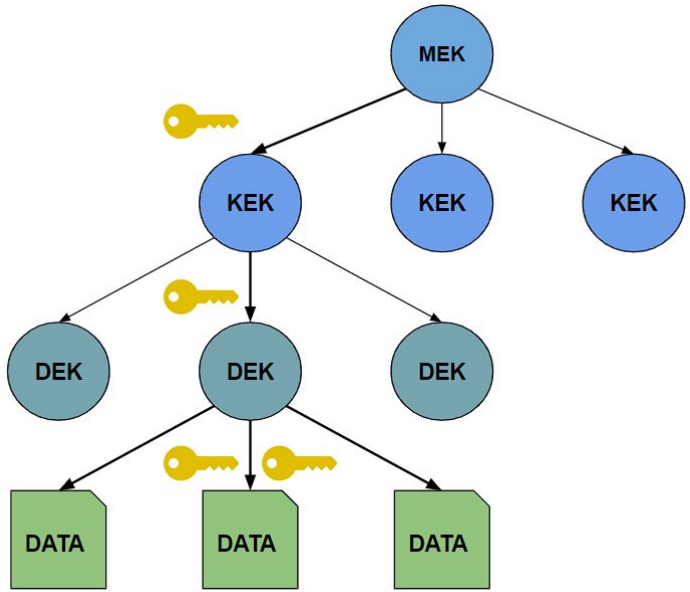


Chiffrement à l'échelle industrielle

Hiérarchie des clés

- Présentation du concept de Hiérarchie de clés
    - DEK chiffre la données, KEK chiffre la DEK, MEK chiffre la KEK

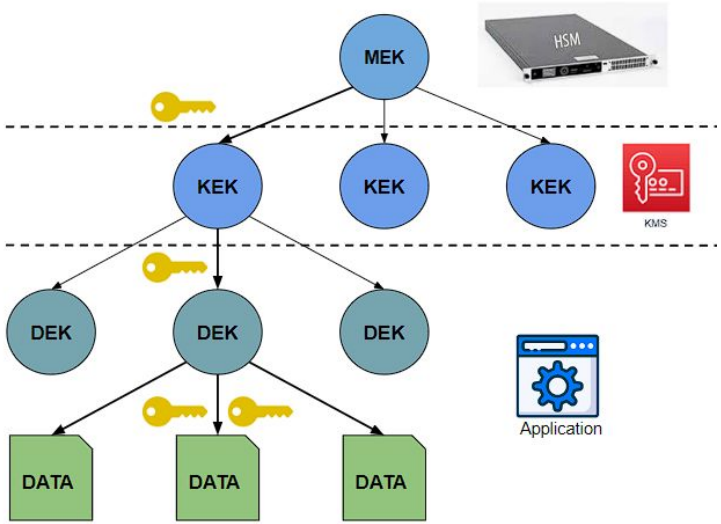
- Segmentation des responsabilités
- Evolutivité
- Crypto-shredding

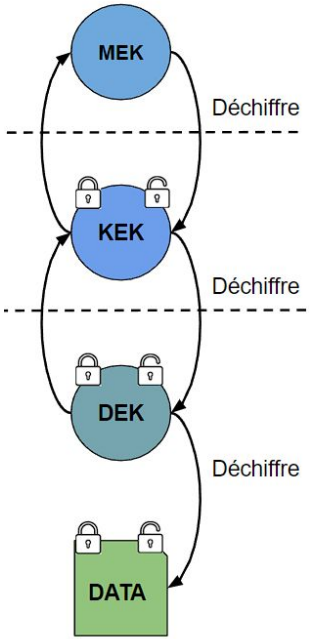


Chiffrement à l'échelle industrielle

Key Management Services (KMS) & Hardware Security Modules (HSM)

- Stockage sécurisée de clés
  - HSM inviolable
  - KMS moins robuste mais plus souple.

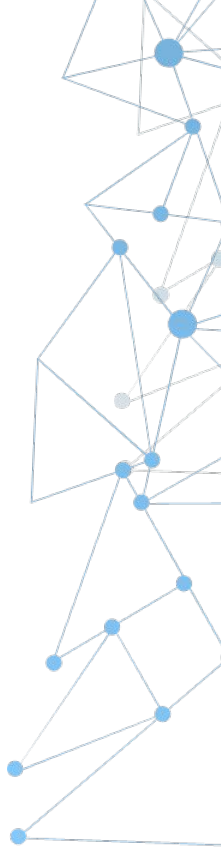




Chiffrement à l'échelle industrielle

Bonnes pratiques

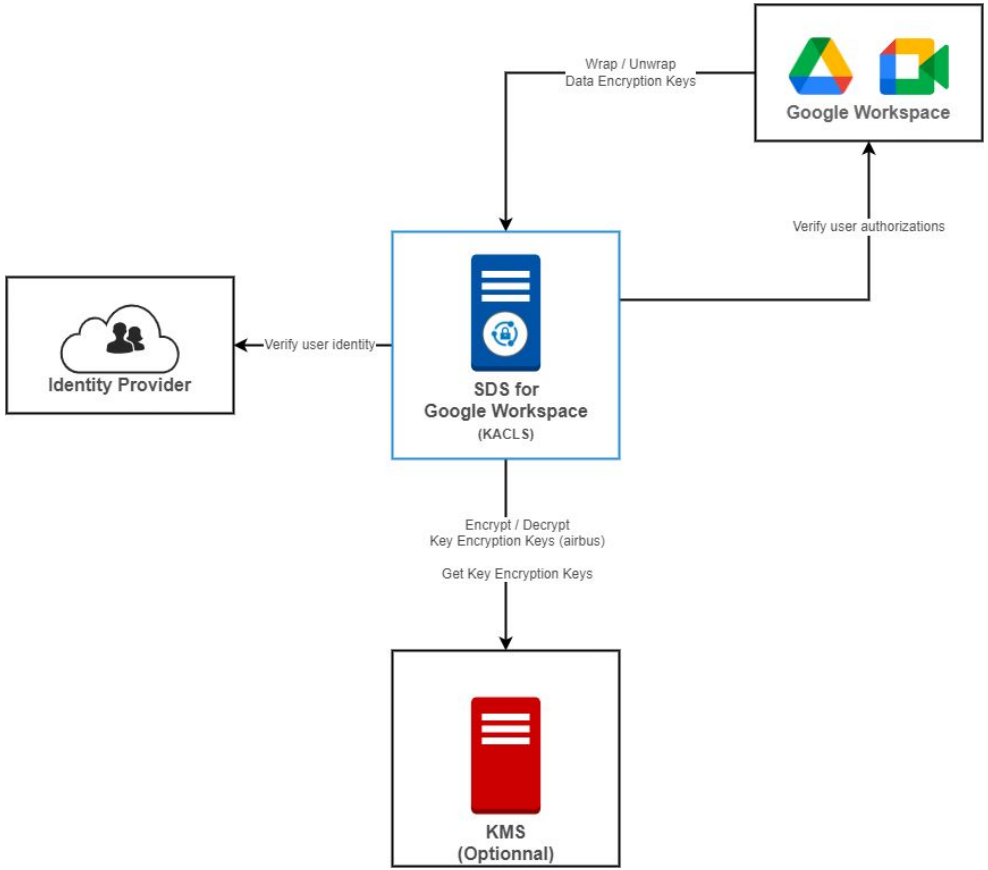
- Utiliser un Algorithme de chiffrement Robuste avec une taille de clé approprié (AES)
- Utiliser les outils appropriés (KMS & HSM)
- Mise en place de rotations régulière des clés
- Une DEK par donnée (Fichier, disque, etc…)
- Une KEK par domaine (Organisation, service, etc…)



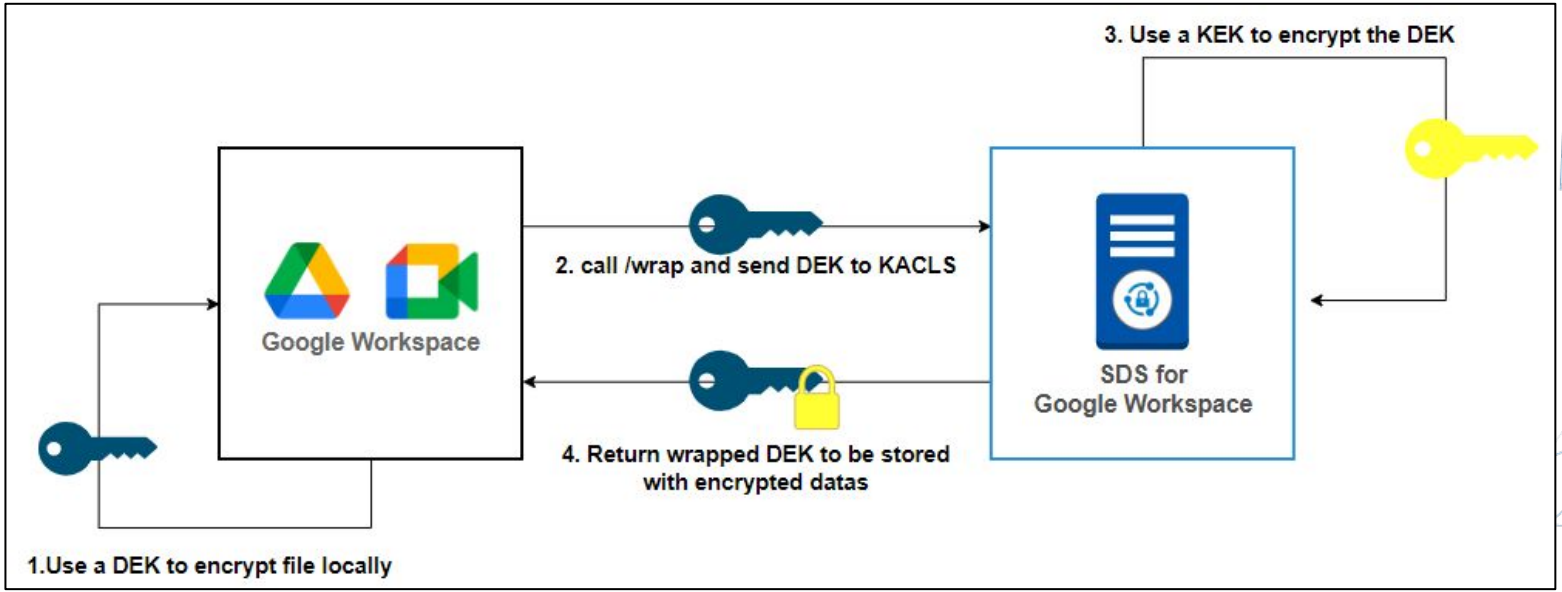
Cas pratique

CSE

Cas pratique – CSE Google Workspace

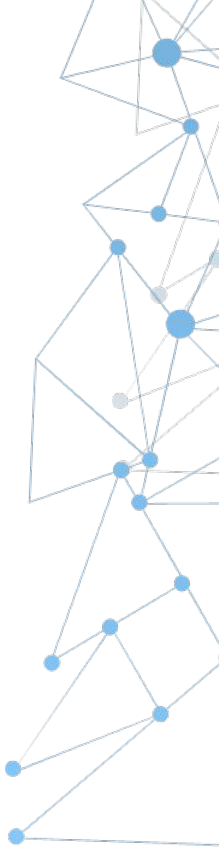


Cas pratique – CSE Google Workspace



Cas pratique – CSE Google Workspace

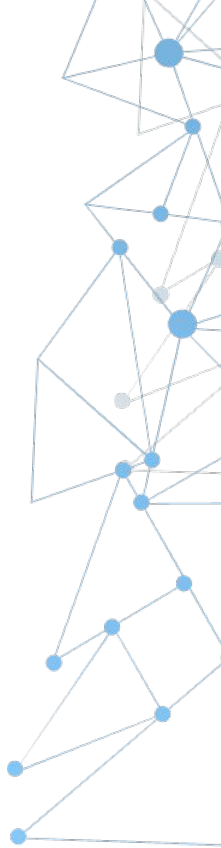
- Enregistrer
  - (Docs, Slides, Meets etc..) chiffrés directement sur la navigateur avec une DEK
  - La DEK est envoyer à un KACLS qui la chiffre (wrap) avec une KEK
  - La DEK chiffré est envoyée au serveurs de Google
- Ouverture
  - La DEK chiffré et le document sont récupérer sur le navigateur
  - La DEK chiffré est envoyer au KACLS qui la déchiffre (unwrap) avec la KEK
  - Le document peut être déchiffré directement sur le navigateur



Cas pratique – CSE Google Workspace

KACLS Stormshield

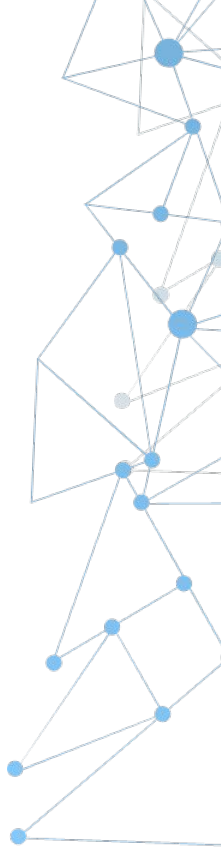
- Problématique de chiffrement à grande échelles
- Produit de sécurité → Développement sécurisée
- Mise en oeuvre de certains concepts DevSecOps



Cas pratique – CSE Google Workspace

Développement sécurisé

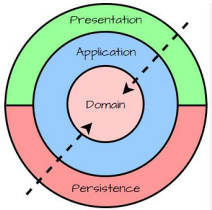
- Plan ❌
- Code ✔️
- Build ✔️
- Test ✔️
- Release ❌
- Deploy ✔️
- Operate ❌
- Monitor ❌

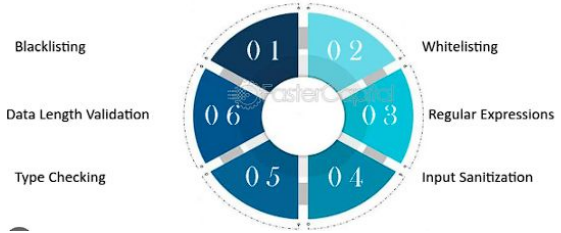


Cas pratique – CSE Google Workspace

Code

- Développement Backend NodeJS





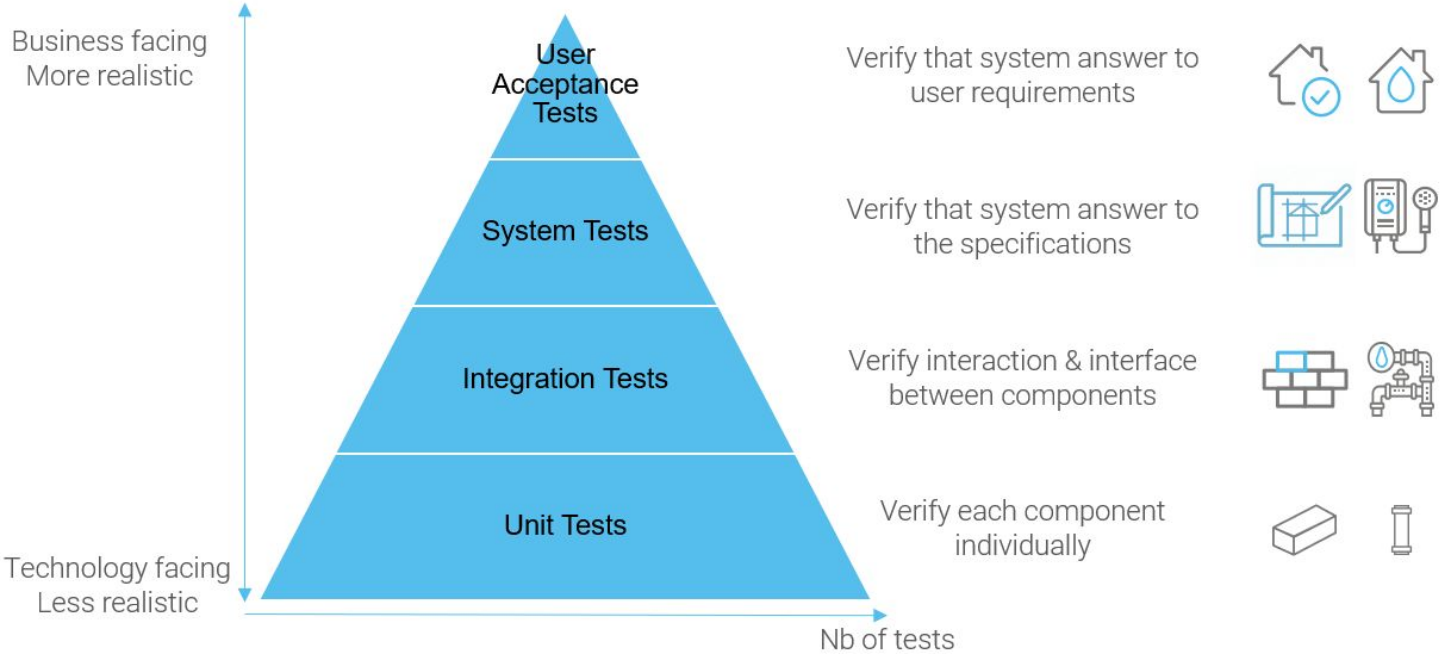
Cas pratique – CSE Google Workspace

Build

- Déploiement SAAS et On-premise

Cas pratique – CSE Google Workspace

Test



Cas pratique – CSE Google Workspace

Deploy

- Hardening

- Secrets Management

mozilla/**sops**

- Kubernetes Security

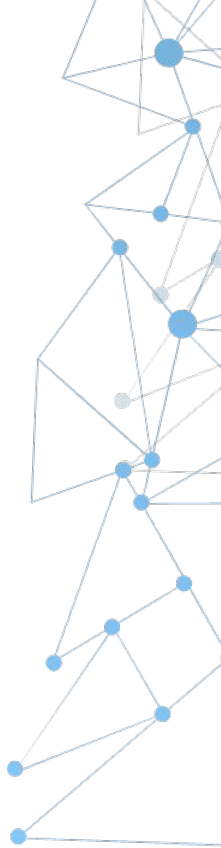
Tendances et Perspectives

dans le monde de la cryptographie

Tendances et Perspectives

Service de chiffrement et chiffrement homomorphique

- Besoin universel
  - Google CSE – Client Side Encryption
  - Google EKM – External Key Manager
  - Microsoft DKE – Double Key Encryption
  - AWS Custom Key Stores
- Adoption de plus en plus présent
- Chiffrement homomorphe
  - Effectuer des opérations sur des données chiffrées sans les déchiffrer
  - Préserver la confidentialité



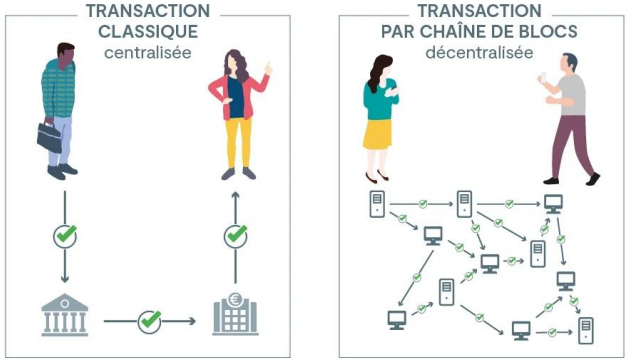
Tendances et Perspectives

Blockchain et Smart Contracts

- Révolution dans la confiance et l'exécution de contrats intelligents

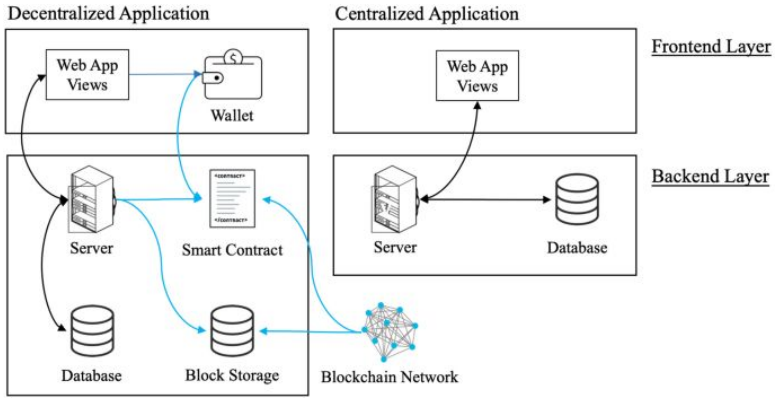
Blockchain

- Immutable
- Décentralisée
- Transparent
- Trustless



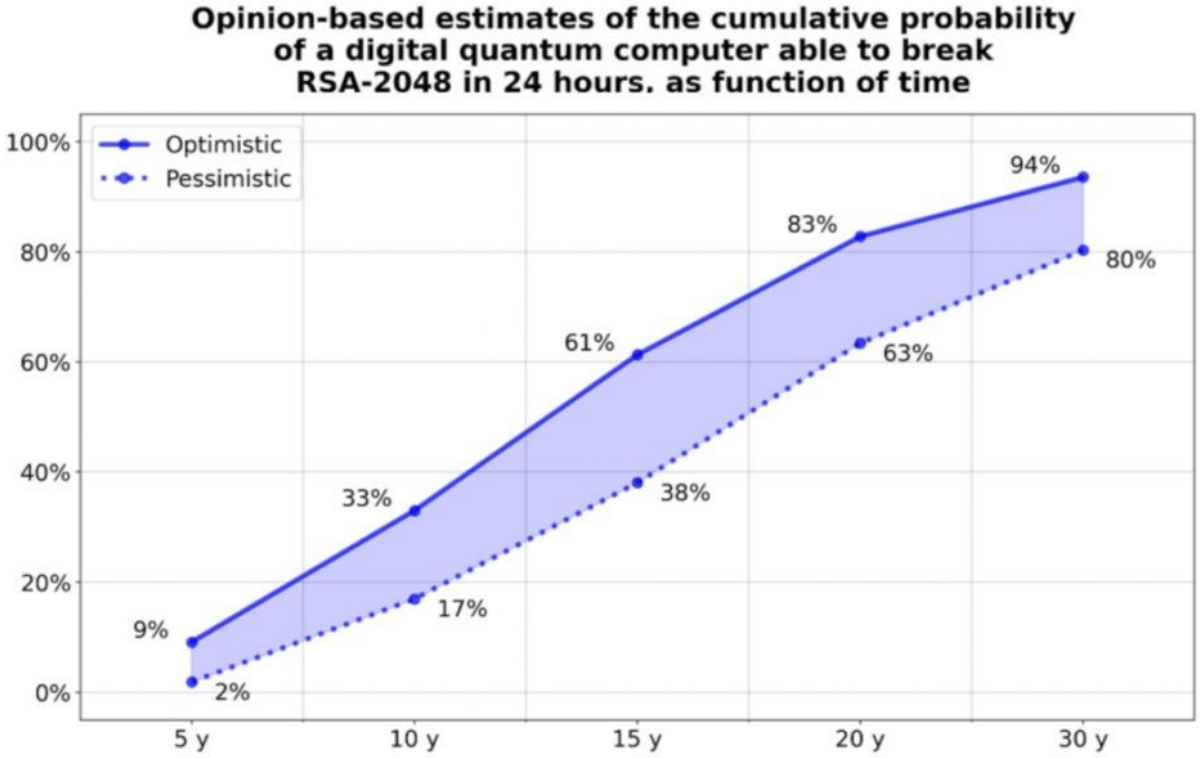
Smart Contract

- version numérique d'un contrat
- automatisation de transactions
- Assure le respect de clauses
- Auditable



Tendances et Perspectives

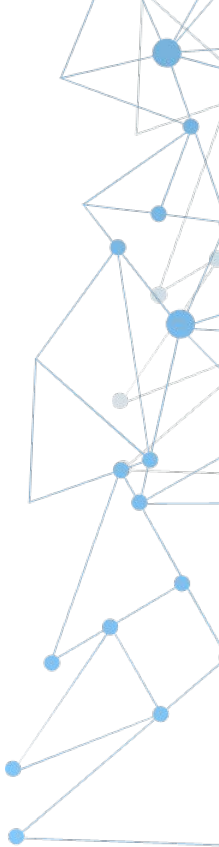
Post-Quantique



Tendances et Perspectives

Post-Quantique

- Préparation à l'ère de l'informatique quantique
- Adoption anticipée des algorithmes de cryptographie supportant les attaques quantiques
    - CRYSTALS Kyber
    - CRYSTALS Dilithium



Thank you

Looking forward to hearing from you

Get in Touch

22, rue du Gouverneur Général Éboué
92130 Issy-les-Moulineaux FRANCE

+33 (0) 9 69 32 96 29

sales@stormshield.eu

www.stormshield.com