Module 6: Sécurité dans Azure DevOps

Introduction à la Sécurité CI/CD

Importance de la sécurité dans le pipeline CI/CD

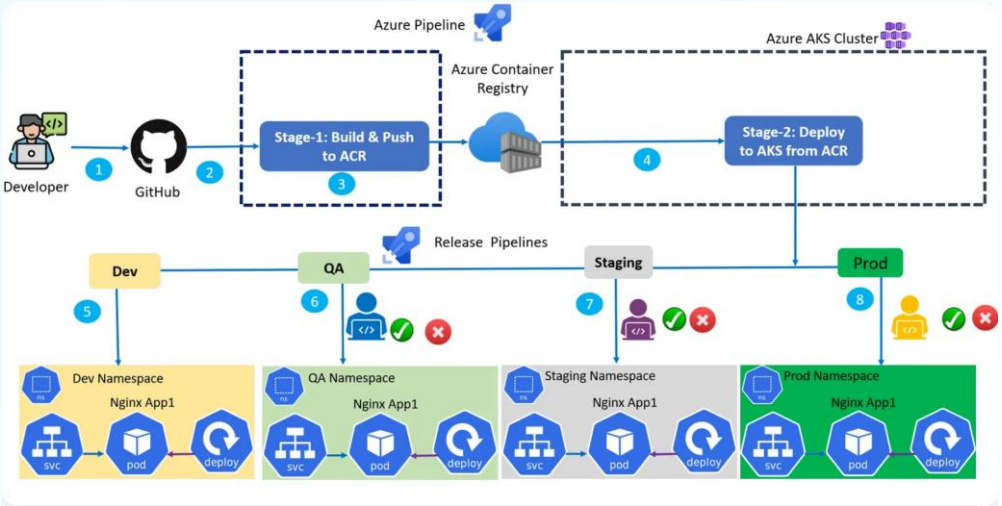
- Prévenir les vulnérabilités dès le début du cycle de développement
- Protéger les actifs et les données sensibles
- Assurer la conformité réglementaire

Menaces courantes dans les pipelines DevOps

- Secrets exposés (clés API, mots de passe)
- Dépendances vulnérables
- Images conteneurs non sécurisées
- Configurations erronées

Approche "Security by Design"

- Intégrer la sécurité à chaque étape du pipeline
- Responsabilité partagée de la sécurité



Module 6: Sécurité dans Azure DevOps

Bonnes Pratiques de Sécurité dans les Pipelines CI/CD

Shift Left Security

Intégrer les contrôles de sécurité le plus tôt possible dans le cycle de développement

Détecter et corriger les problèmes de sécurité avant qu'ils ne deviennent coûteux

Automatisation de la Sécurité

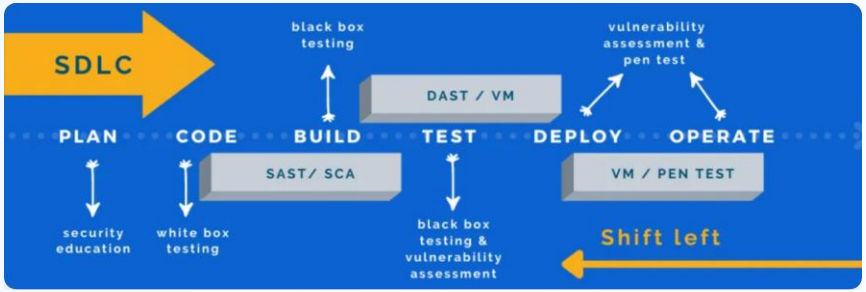
Utiliser des outils automatisés pour l'analyse statique du code (SAST), l'analyse dynamique (DAST), l'analyse des dépendances (SCA)

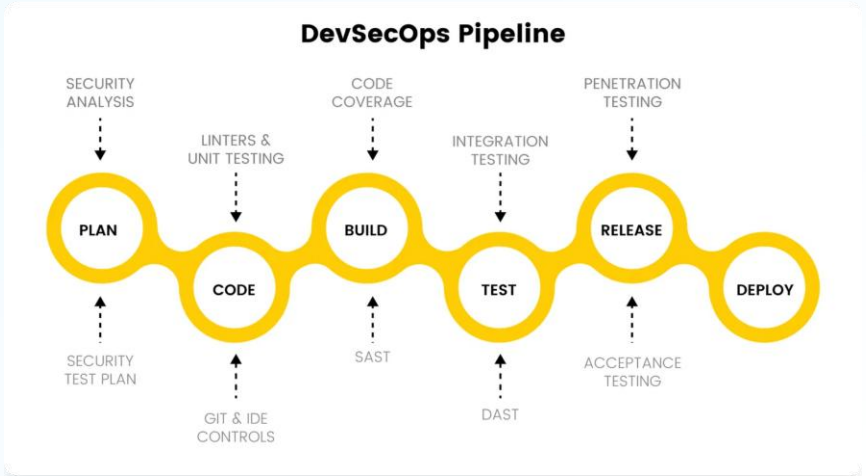
Intégrer ces outils directement dans les pipelines Azure DevOps

Principes de Moindre Privilège

Accorder uniquement les permissions nécessaires aux utilisateurs et aux services

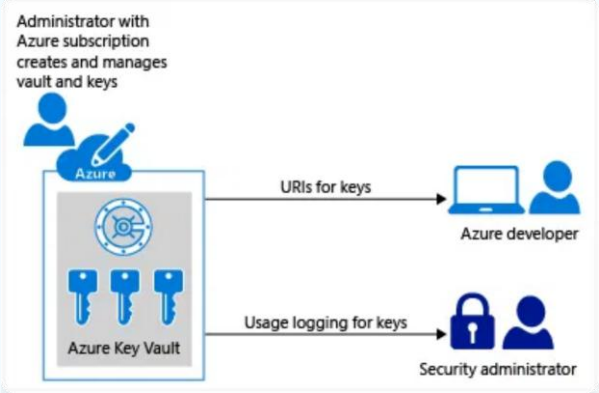
Réduire la surface d'attaque





Module 6: Sécurité dans Azure DevOps

Gestion des Secrets avec Azure Key Vault



Qu'est-ce qu'Azure Key Vault ?

Service cloud pour stocker et gérer de manière sécurisée les clés cryptographiques, les certificats et les secrets

Élimine le besoin de stocker les secrets dans le code ou les fichiers de configuration

Avantages de Key Vault dans CI/CD

Centralisation et sécurisation des secrets

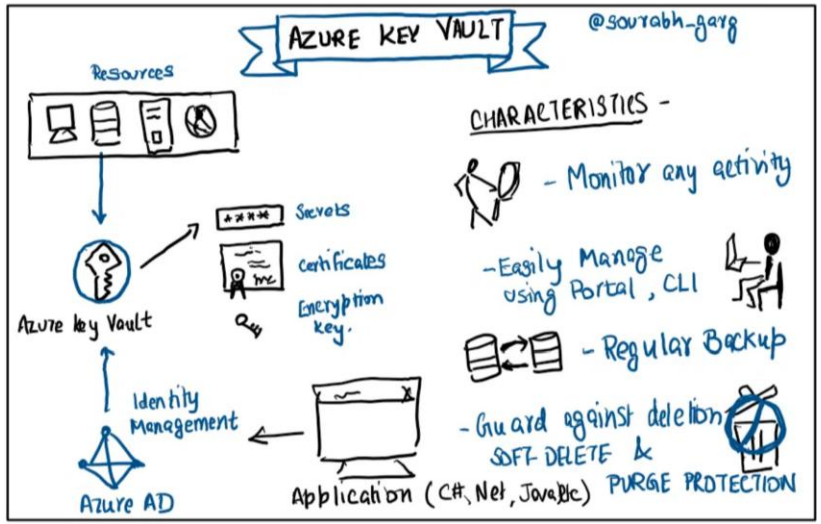
Rotation automatique des clés

Audit et surveillance de l'accès aux secrets

Intégration d'Azure Key Vault avec Azure Pipelines

Utilisation de tâches de pipeline dédiées pour récupérer les secrets

Accès aux secrets via des variables de pipeline



Module 6: Sécurité dans Azure DevOps

Contrôle d'Accès et Connexions de Service

Gestion des identités et des accès (IAM)

Utilisation Entra ID (Azure Active Directory) pour l'authentification et l'autorisation

Principes du moindre privilège pour les utilisateurs et les services

Connexions de service dans Azure DevOps

Mécanisme sécurisé pour connecter Azure DevOps à des services externes (Azure, GitHub, etc.)

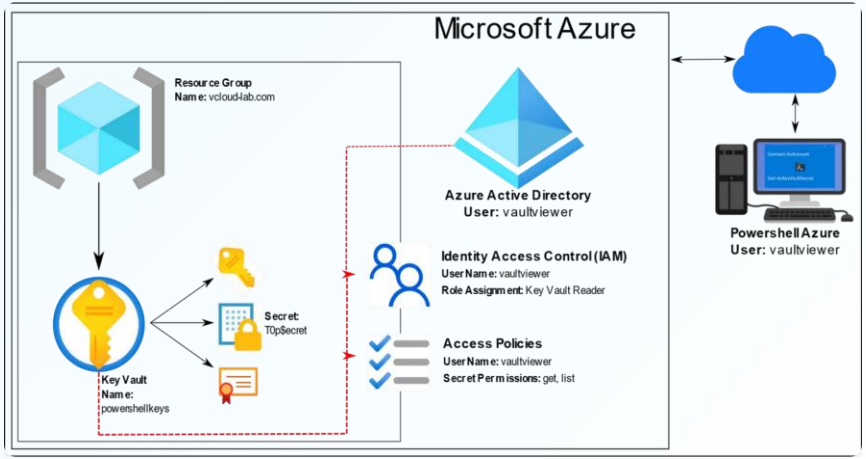
Types de connexions de service (Azure Resource Manager, Generic, etc.)

Bonnes pratiques pour les connexions de service

Utiliser des identités de service managées (MSI) lorsque possible

Limiter les permissions des connexions de service au strict nécessaire

Rotation régulière des identifiants



Module 6: Sécurité dans Azure DevOps

Analyse de la Sécurité Statique (SAST)

Qu'est-ce que le SAST ?

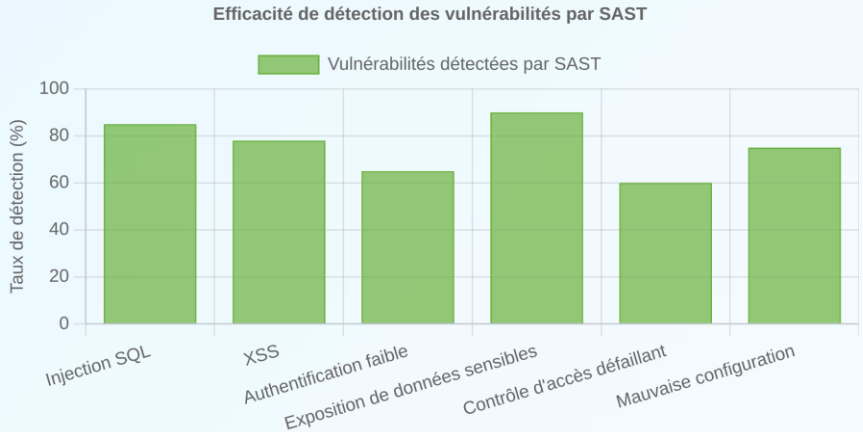
Analyse du code source, bytecode ou binaire sans l'executer
Détection de vulnérabilités courantes (OWASP Top 10, CWE)

Outils SAST populaires

SonarQube, Checkmarx, Fortify, Snyk Code

Intégration SAST dans Azure Pipelines

Ajout de tâches de pipeline pour exécuter des analyses SAST
Blocage des builds en cas de vulnérabilités critiques détectées



Feature	SAST (Static Application Security Testing)	DAST (Dynamic Application Security Testing)	SCA (Software Composition Analysis)
Approach	Analyzes source code before execution	Tests a running application	Scans for vulnerabilities in open-source components
Timing	Early in the software development lifecycle (SDLC)	Often later in the SDLC, on a running application	Throughout the SDLC
Requires Code Access?	Yes	No	No
Focus	Finding code-level vulnerabilities	Finding runtime vulnerabilities and configuration issues	Identifying risks in third-party libraries and components

Module 6: Sécurité dans Azure DevOps

Analyse de la Sécurité Dynamique (DAST)

Qu'est-ce que le DAST ?

Analyse des applications en cours d'exécution

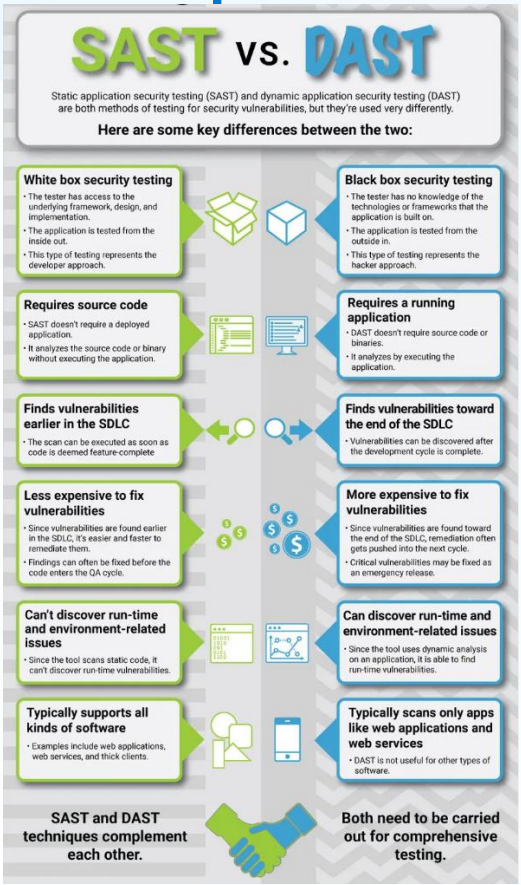
Simule des attaques externes pour trouver des failles

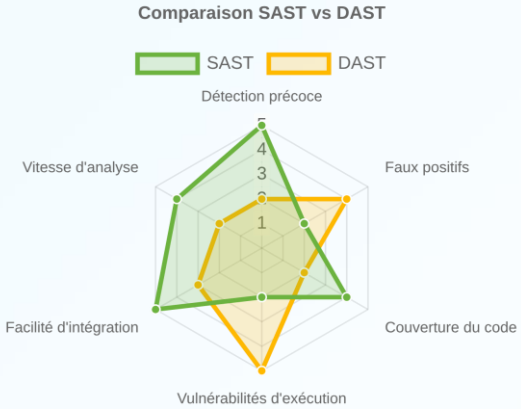
Outils DAST populaires

OWASP ZAP, Acunetix, Burp Suite

Intégration dans Azure Pipelines

Exécution après déploiement en environnement de test
Intégration des rapports de vulnérabilités





Module 6: Sécurité dans Azure DevOps

Analyse de la Composition Logicielle (SCA)

Qu'est-ce que le SCA ?

Identification des composants open source et tiers

Détection des vulnérabilités connues (CVE) et des problèmes de licence

Outils SCA populaires

Snyk, Mend (WhiteSource), Black Duck

Intégration SCA dans Azure Pipelines

Scan des dépendances lors du build ou du déploiement

Blocage des builds si des vulnérabilités critiques sont détectées