Open Source is HOT

3 au 6 juillet 2017

SophiaConf

Le cycle azuréen de conférences Open Source

by TelecomValley Animateur Azuréen du Numérique

Elastic Detector ®

SophiaConf
Sécurité des Micro services

Donnat Frédéric – Dir. Technique et CoFondateur

03/07/2017

SECLUD IT
AHEAD OF SECURITY

SecludIT

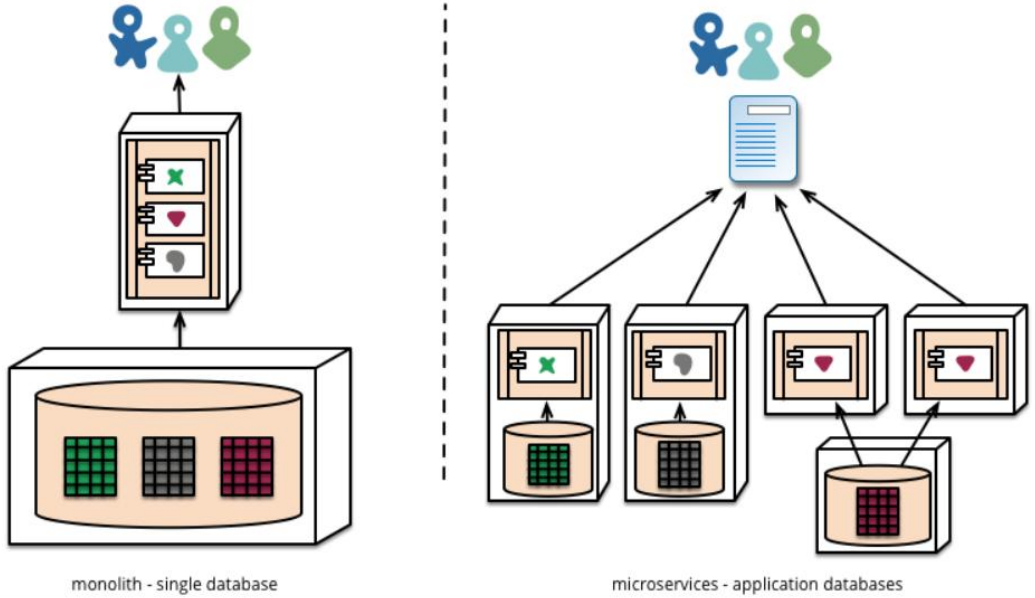
- SecludIT est un Editeur français qui aide les entreprises, les hébergeurs ou infogéreurs à sécuriser leurs infrastructures informatiques.

- Notre objectif est de démocratiser les meilleures techniques préventives de sécurité informatique.

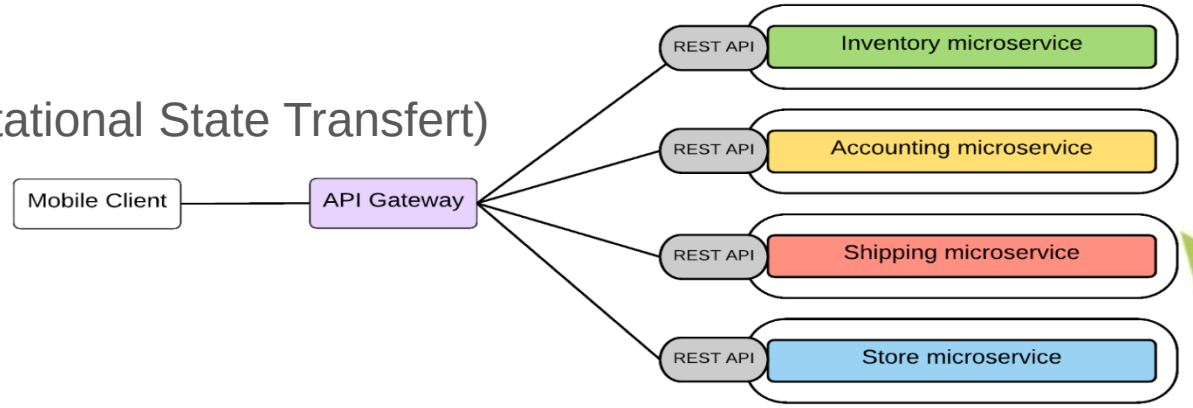
- SecludIT : acteur reconnu de l'industrie!
  - Partenariats avec les acteurs majeurs du cloud et de la virtualisation tel qu'Amazon Web Services, Azure, OpenStack, CloudStack, VMware

Micro-services

- Monolithique vs Micro services

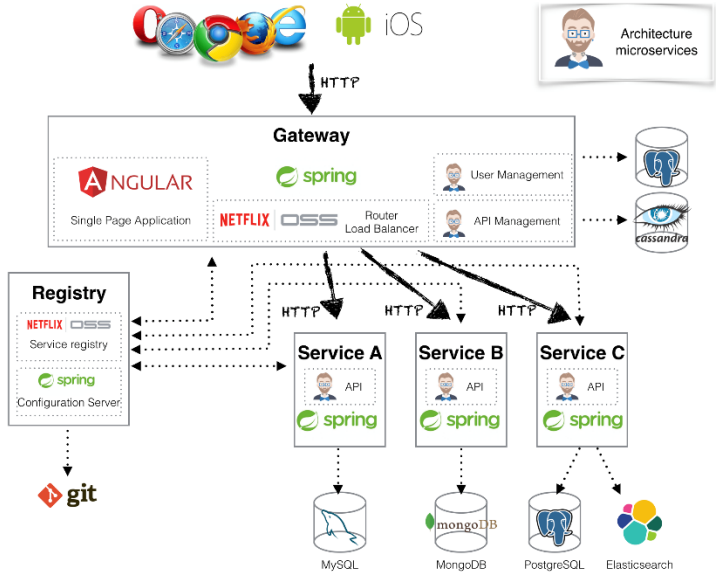


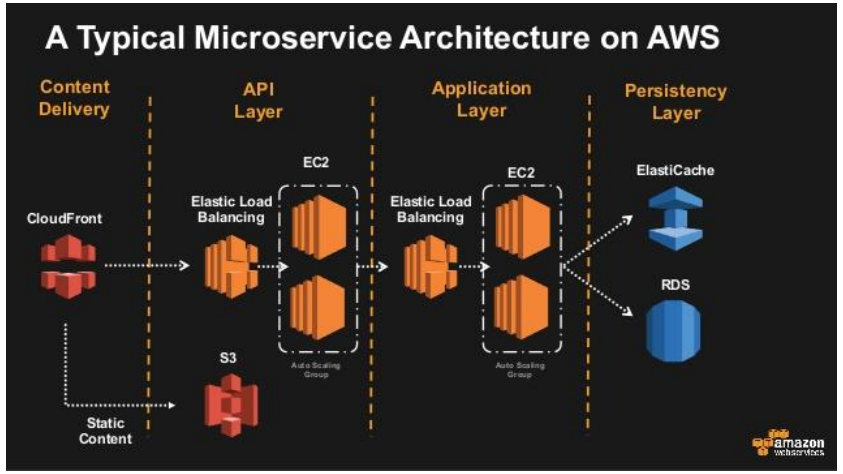
- Micro service : Composant
  - 1 fonctionnalité
  - 1 processus
  - HTTP REST (Representational State Transfert)
  - Langage propre



1 – Micro services & APIs

- Isolation réseau ou cloisonnement
- Communications sécurisées
- Authentification
- Autorisation, Propagation des autorisations
- Interaction entre services
- Restriction entre service ou entre utilisateurs de service
- Logs



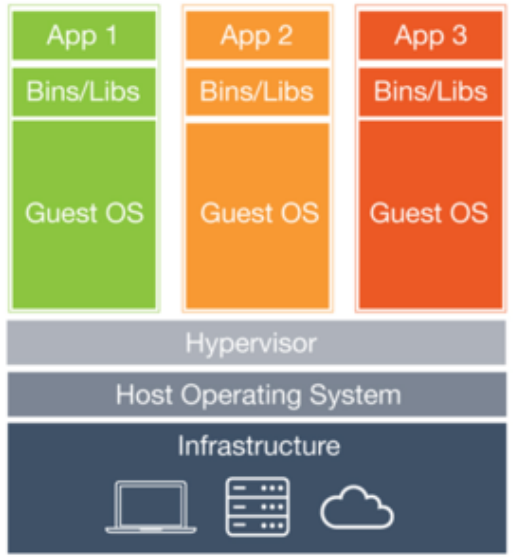


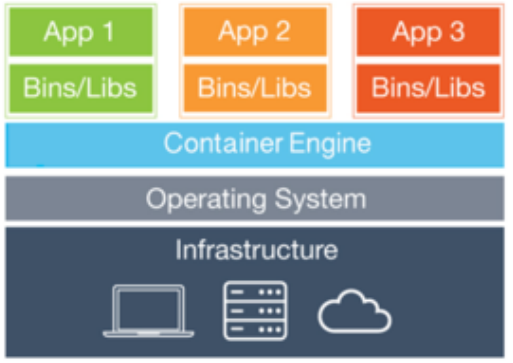
2 – Framework

- Partage de base de données à travers le système
- Principe des « Moindres Privilèges »
- Chiffrement des données
  - Stockage
  - Transfert
- Accès « par service » vs « par utilisateur » :
  - Chaque service à son propre accès
  - Accès dérivé des accès utilisateurs
- Protection des clés d’accès
- Logs

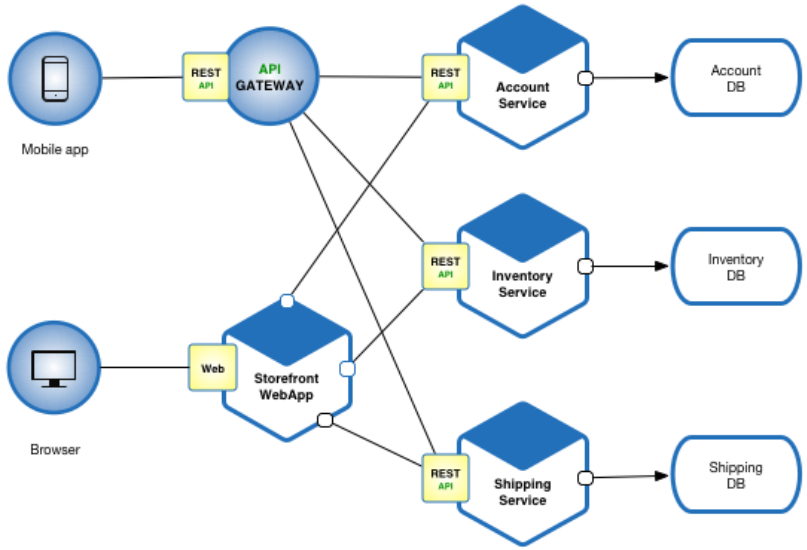
3 – Le coin DevOps

- Ou résident les micro services ?
  - Containers, VMs, …
- Interaction entre les systèmes services





- Authentification, autorisation
- Communication sécurisées
- Chiffrement des données
- Stockage des clés d'accès
- Durcissement des systèmes



4 – Sécurité des Micro services & APIs

- OWASP

A10-Underprotected APIs

Modern applications often involve rich client applications and APIs, such as JavaScript in the browser and mobile apps, that connect to an API of some kind (SOAP/XML, REST/JSON, RPC, GWT, etc.). These APIs are often unprotected and contain numerous vulnerabilities.

TOP10 Risk OWASP :

A3-Cross-Site Scripting (XSS)

A6-Sensitive Data Exposure

A7-Insufficient Attack Protection

A9-Using Components with Known Vulnerabilities

Components, such as libraries, frameworks, and other software modules, run with the same privileges as the application. If a vulnerable component is exploited, such an attack can facilitate serious data loss or server takeover. Applications and APIs using components with known vulnerabilities may undermine application defenses and enable various attacks and impacts.

5 – Scan de Vulnérabilités

- Scan réseau via « nmap »
  - Détection des équipements sur le réseau
  - Détection des services sur les composants du réseau

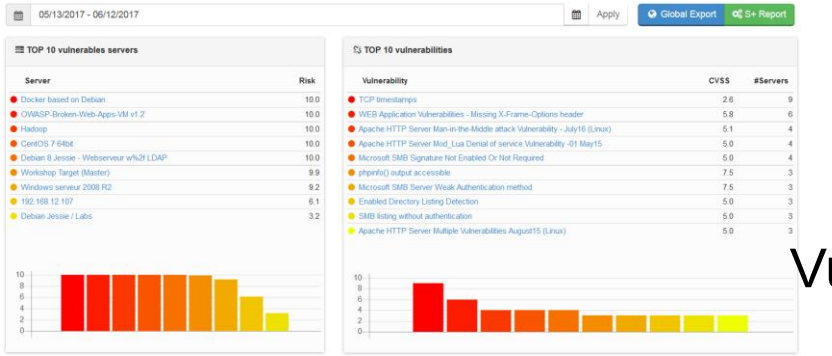
- Scan de vulnérabilité
  - Détection des vulnérabilités CVE
  - Détection des problèmes de configuration
  - Durcissement des serveurs CIS (Center for Internet Security)

Common Vulnerabilities and Exposures
The Standard for Information Security Vulnerability Names

Center for Internet Security®

- Scan Web via outils « OWASP »
  - Détection des failles relatives aux applications Web
  - OWASP Zed Attack Proxy

6 – Sécurité dans le cycle de SecDevOps



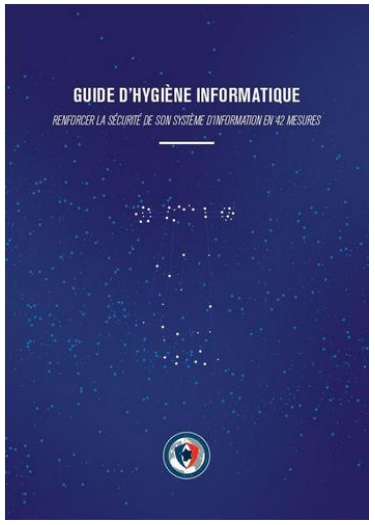
Scans de Vulnérabilités

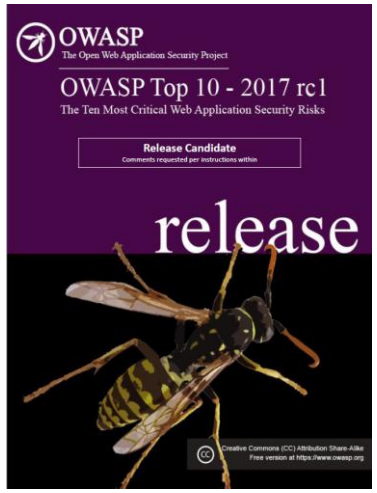
Tests d'Intrusions

KALI BY OFFENSIVE SECURITY

EXPLOIT DATABASE

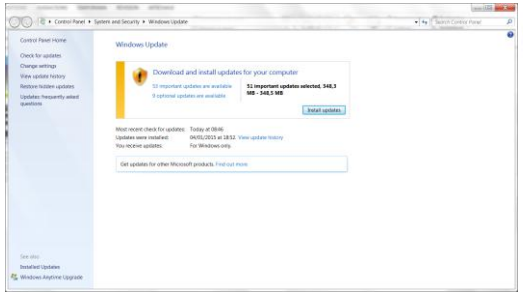
metasploit





Remédiation

Mise à Jour



7 – Bénéfices

- Réduire la « fenêtre » de faiblesse du système d'information (en terme de sécurité)
- Minimiser l'impact opérationnel
- Détection de problème reproductible
- Gain de temps par priorisation et planification des tâches correctives : Indicateurs de Risque
- Réduction des coûts
  - Quelle perte pour un arrêt de production ?
  - Meilleure rentabilité des Auditeurs

Références

- Sécurité des Micro services : Les questions de sécurité à se poser
  http://www.grahamlea.com/2015/07/microservices-security-questions/

- OWASP : Projet OWASP TOP10
  https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project

- OWASP : Sécurité REST
  https://www.owasp.org/index.php/REST_Security_Cheat_Sheet

- OWASP : Sécurité Web Service
  https://www.owasp.org/index.php/Web_Service_Security_Cheat_Sheet

QUESTIONS ?

Essayez et Adoptez Elastic Detector !