Jug Summer Camp

-enjoy it-

La sécurité dès la conception du projet

Speaker : David Aparicio - @dadideo

SERLI

POITOU CHARENTES

David Aparicio

@dadideo

15/ DD INSA de Lyon / UNICAMP (Brésil)

Facebook Open Academy / MIT AppInventor

17/ Dev(Sec)Ops @ AMADEUS (Nice, 2 ans)

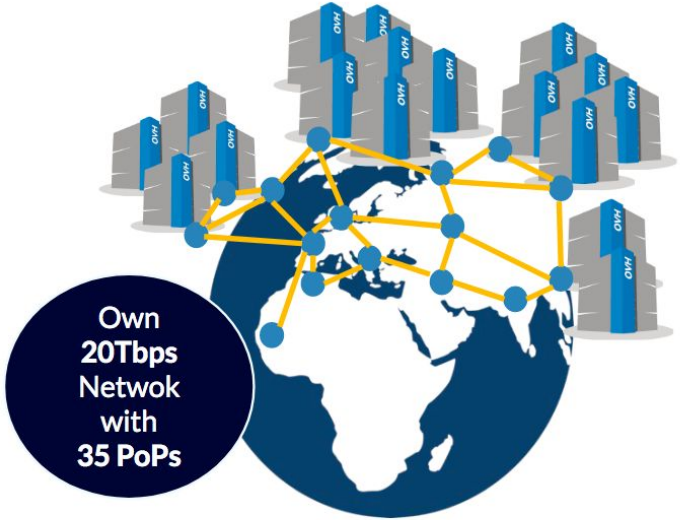
19/ Data(Sec)Ops @ OVHcloud (Lyon, 2 ans)

OVHcloud

OVHcloud: Un leader européen

200k Private cloud VMs running

Dedicated IaaS Europe



30 Datacenters

Hosting capacity :
1.3M Physical Servers

360k
Servers already deployed

> **1.3M** Customers in **138** Countries

OVHcloud: 4 univers de produits

Domain / Email
- Domain names, DNS, SSL, Redirect
- Email, Open-Xchange, Exchange
- Collaborative Tools, NextCloud

PaaS for Web
- Mutu, CloudWeb
- Plesk, CPanel
- PaaS with Platform.sh

Virtual servers
- VPS, Dedicated Server

SaaS
- Wordpress, Magento, Prestashop
- CRM, Billing, Payment, Stats
- MarketPlace

Support, Managed
- Support Basic
- Support thought Partners
- Managed services

Standalone, Cluster
- General Purpose
- SuperPlan
- Game
- Virtualization
- Storage
- Database
- Bigdata
- HCI
- AI
- VDI Cloud Game
- Network

T2 >20e
T3 >80e
T4 >300e
T5 >600e
12KVA /32KVA

VPS aaS
- pCC DC
- Virtuozzo Cloud

Wholesales
- IT Integrators, Cloud Storage,
- CDN, Database, ISV, WebHosting
- High Intensive CPU/GPU,

Encrypt
- KMS, HSM
- Encrypt (SGX, Network, Storage)

Compute
- VM
- Baremetal
- K8S, IA IaaS
- PaaS for DevOps

Storage
- File, Block, Object, Archive

Databases
- SQL, noSQL, Messaging,
- Dashboard

Network
- IP FO, NAT, LB, VPN, Router,
- DNS, DHCP, TCP/SSL Offload

Security
- IAM, MFA, Encrypt, KMS

IA, DL
- Standard Tools for AI, AI Studio,
- IA IaaS, Hosting API AI

Bigdata, ML, Analytics
- Datalake, ML, Dashboard

Hosted Private Cloud

VMware
- SDDC, vSAN 1AZ / 2AZ
- vCD, Tanzu, Horizon, DBaaS,
- DRaaS

Nutanix
- HCI 1AZ / 2AZ, Databases,
- DRaaS, VDI

OpenStack
- IAM, Compute (VM, K8S)
- Stortage, Network, Databases

Storage
- Ontap Select, Nutanix File
- OpenIO, MinIO, CEPH
- Zerto, Veeam, Atempo

AI
- ElementAI, HuggingFace,
- Deepopmatic, Systran,
- EarthCube

Bigdata / Analitics / ML
- Cloudera over S3, Dataiku,
- Saagie, Tableau,

Hybrid Cloud
- vRack Connect, Edge-DC, Private DC
- Dell, HP, Cisco, OCP, MultiCloud

Secured Cloud
- GOV, FinTech, Retail, HealtCare

Pitch

Salut à toi jeune développeur(euse) !
Alors si aujourd'hui je me permets de te contacter, c'est pour une raison très simple:

Savais-tu que 95% des failles de sécurité sont dues à une erreur humaine ?

Pitch

Alors est-ce que tu veux en faire parti ?
Il faut que tu te poses les bonnes questions.

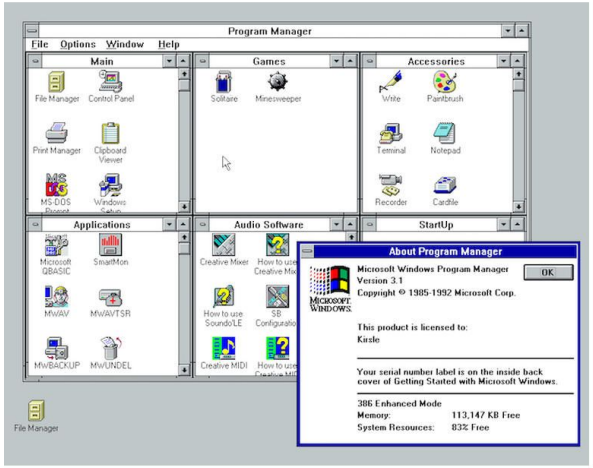
Moi je pense la question elle est vite répondue

https://www.zdnet.com/article/a-23-year-old-windows-3-1-system-failure-crashed-paris-airport/

A 23-year-old Windows 3.1 system failure crashed Paris airport

Some of the most important networks and systems today are woefully outdated. And that isn't always a bad thing.

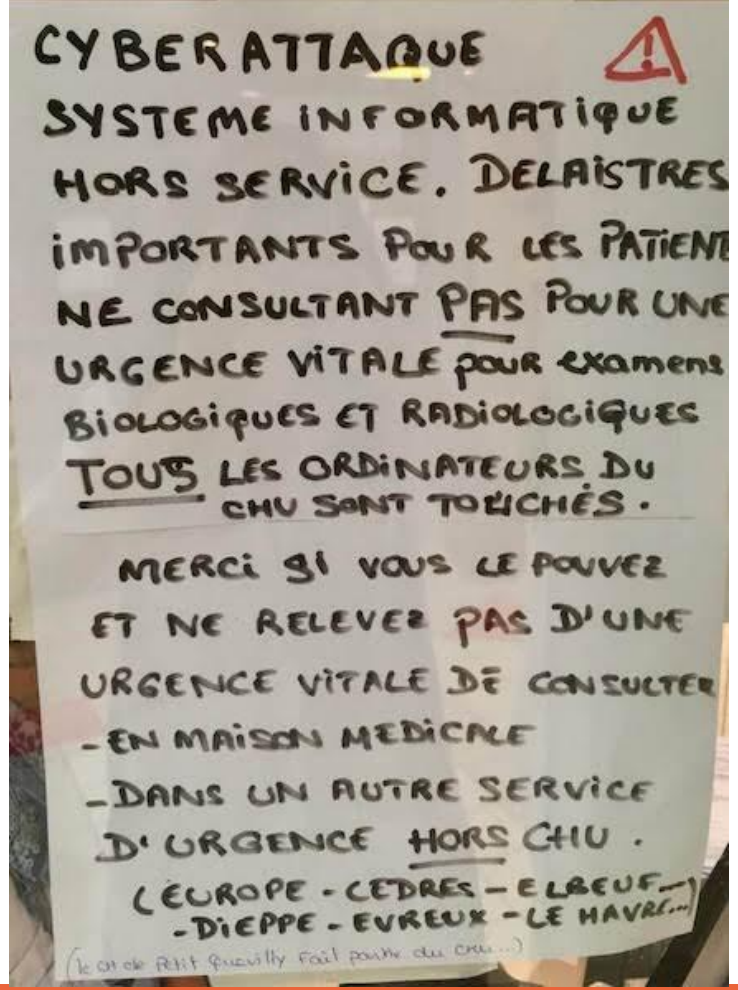
By Zack Whittaker for Zero Day | November 16, 2015 -- 21:04 GMT (21:04 GMT) | Topic: Security



(Image: Imgur)

Source : ZDNet.com

Pour éviter cela



Plus d'infos : [Thread @zigazou]

Plan

- Définition
- Best Practices
- Outils
- Scénarios
- Q/A

Sécurité dès la conception

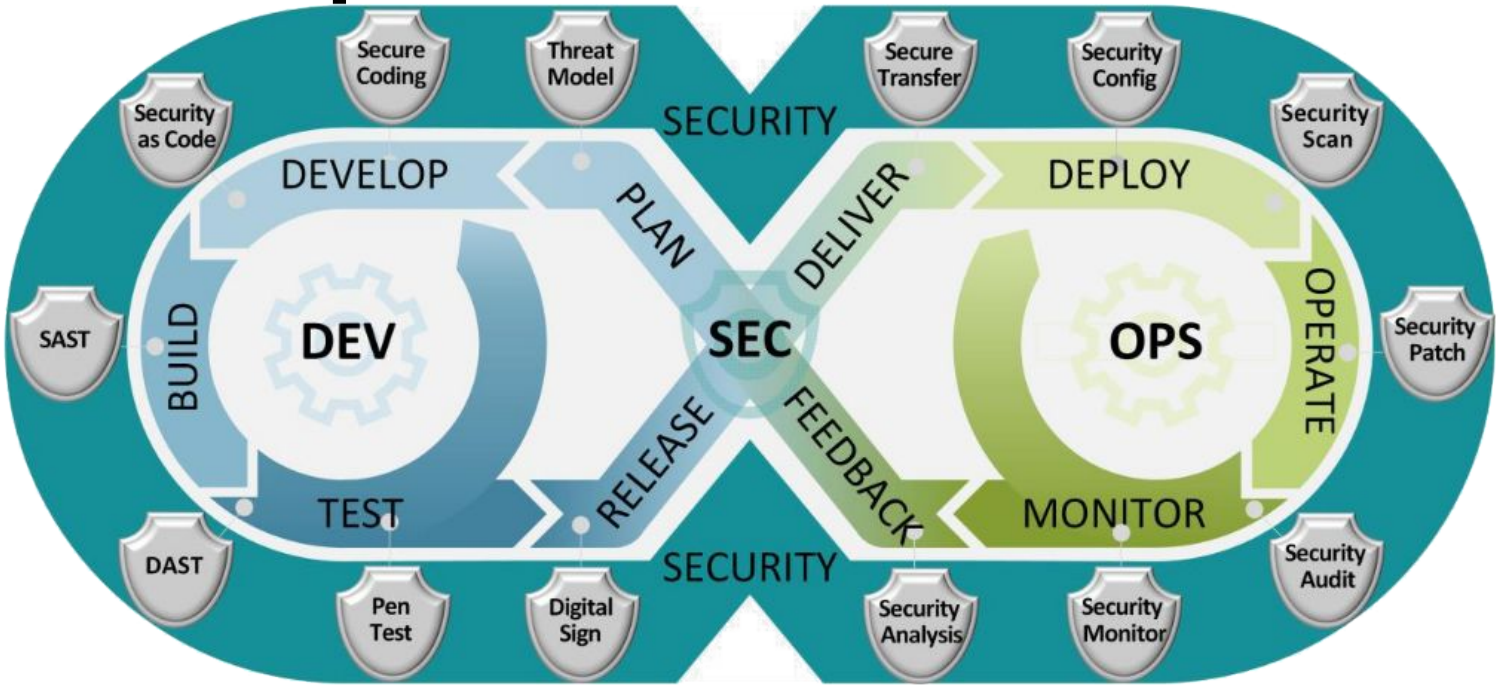
95/ SdD-"Privacy By Design"

97/ Loi allemande

10-12/ Congrès EU

2016/679/ GDPR

DevSecOps



Source : dodcio.defense.gov

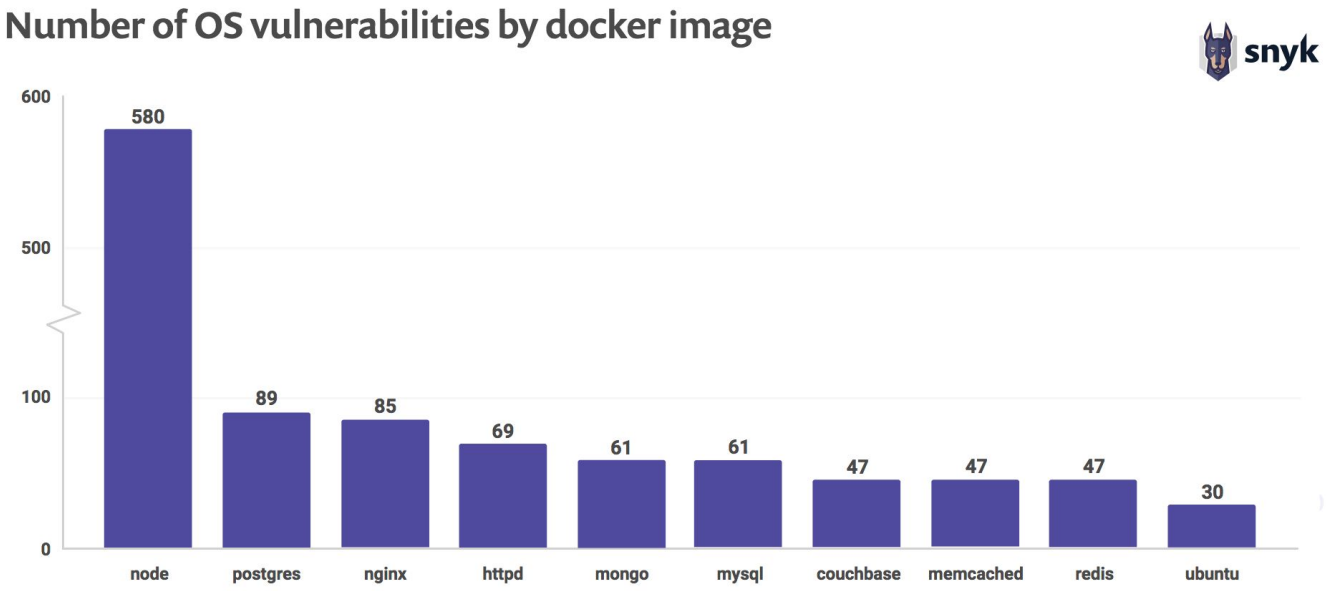
Pas copier-coller `StackOverFlow`

98% snippets sur la sécurité/crypto sont *insecures*

Fisher et al., 2017; Nadi et al., 2016; Das et al., 2014

Prevent cryptographic pitfalls by design

Attention avec Docker



Source : [The state of open source security – 2019]

Attention avec vos dépendences

Open Source Security report

- 78% of vulnerabilities are found in indirect dependencies

Source : [The state of open source security – 2019]

Attention avec vos dépendences

PCWorld
FROM IDG

Start Searching

NEWS | REVIEWS | HOW-TO | VIDEO | DEALS | BUSINESS | LAPTOPS | SMARTPHONES | HARDWARE | SECURITY | SOFTWARE | GADG

Privacy | Encryption | Antivirus

Home / Internet

NEWS

Failure to patch known ImageMagick flaw for months costs Facebook $40k

A researcher found that Facebook was still vulnerable to the ImageTragick exploit months after it was disclosed

By Lucian Constantin
CSO Senior Writer, IDG News Service | JAN 18, 2017 12:06 PM PST

Source : PCWorld - Remote Code Execution Exploit (Write-up)

Bonnes pratiques

- Principe de moindre privilège !root
- Diminuer surface d’attaque (scratch, distroless)
- Pas de secrets dans les Docker images
- Pas de données sensibles dans les GUI
- Ne pas afficher de stacktrace (pas debug)
- Ni de version/nom de framework
- Vérifier les entrées/sorties (injection/XSS)
- Mettre à jour infra/docker images (CI/CD|GitOps)

PaaS (BUILD/RUN) 🇪🇺 OVHcloud/CleverCloud

Open Web Application Security Project

Security by Design Principles by OWASP

1. Minimize attack surface area
2. Establish secure defaults
3. Principle of least privilege
4. Principle of defense in depth
5. Fail securely
6. Don’t trust services
7. Separation of duties
8. Avoid security by obscurity
9. Keep security simple
10. Fix security issues correctly

Source : OWASP

Prendre du recul / code

Security by design in practice [edit]

Many things, especially input, should be distrusted by a secure design. A fault-tolerant program could even distrust its own internals.

Two examples of insecure design are allowing buffer overflows and format string vulnerabilities. The following C program demonstrates these flaws:

```c
#include <stdio.h>

int main()
{
    char a_chBuffer[100];

    printf("What is your name?\n");
    gets(a_chBuffer);
    printf("Hello, ");
    printf(a_chBuffer);
    printf("!\n");

    return 0;
}
```

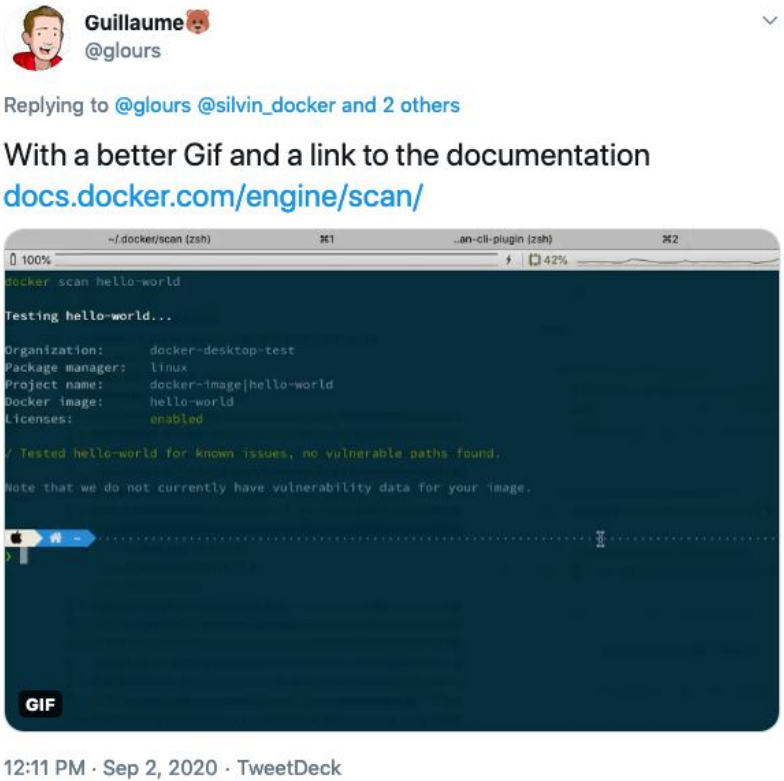
Source : Deprecated code

«David, c'est quand que tu vas mettre des paillettes dans ma vie ?»

Outils

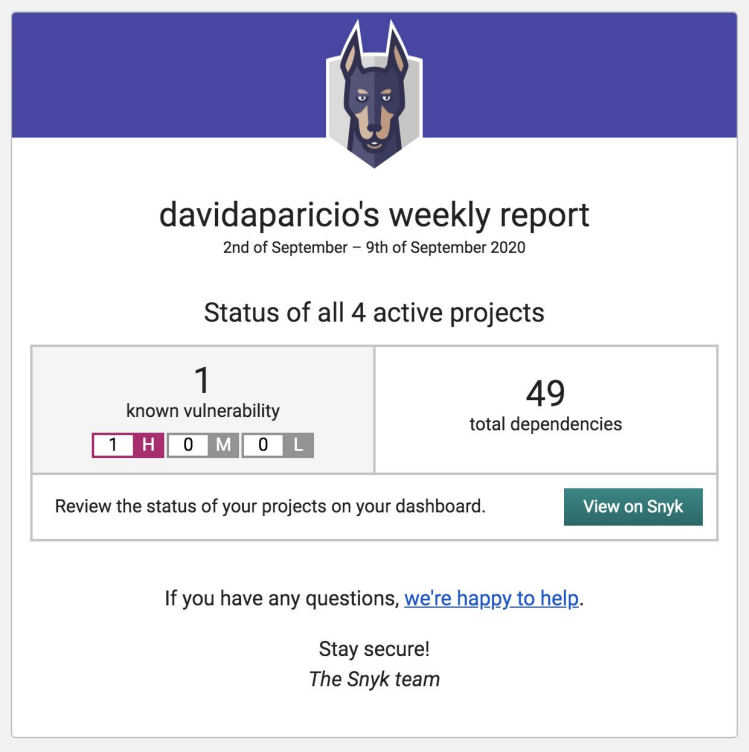
- linter/npm-audit (Code), SonarQube (QA), Gitlab SAST /Argo/GitHub (CI), Saucs/Clair/Anchore/Dagda (CVE),
- OpenSCAP (Audit), Cilium (Network), gVisor/Kata (Sandbox), Istio/maesh (SSL), Notary (Sign.),
- Falco (K8s Monitor), 42Crunch (API Scan), Burp Suite /SuperTruder/ffuf (Vuln.Web), OWASP ZAP (Proxy),
- GitGuardian (Secret), Parrot, Kali, RedHat (OS), YesWeHack, Yogosha (Bounty)

Docker CLI



Source : [Vulnerability scanning - Docker Documentation]

Snyk



Source : Email report

Sonar

```
246  if (Provider.class == roleTypeClass) {
247      Type providedType = ReflectionUtils.getLastTypeGenericArgument(dependen
248  2 Class providedClass = 1 ReflectionUtils.getTypeClass(providedType);
249
250      if (this.componentManager.hasComponent(providedType, dependencyDescript
251          || 3 providedClass.isAssignableFrom(List.class) || providedClass.
```

A "NullPointerException" could be thrown; "providedClass" is nullable here.

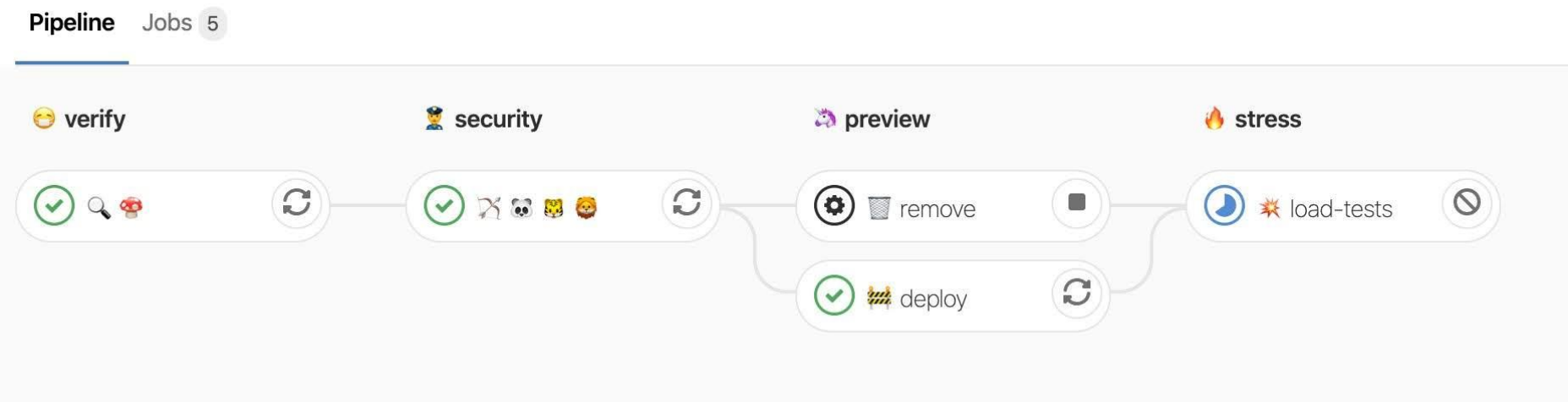
Bug Major cert, cwe

```
252          continue;
253      }
```

			New code Since last release	
Reliability				
Bugs	2	B	1	B
Security				
Security Vulnerabilities	0	A	0	A
Security Hotspots	39	-	0	-
Maintainability				
Technical Debt	6 days	C	0	A
Code Smells	319	-	0	-

Source : [Sonar website]

CI/CD



Source : https://twitter.com/k33g_org/

Falco

- Runtime detection
- Alerts

Falco

Build	Run	Respond
• Image Scanning • Configuration Validation	• Runtime prevention • Automated policy creation using ML • Policy editor and rules library • Automatic remediation • Falco Tuning	• Incident Response • Forensics • Audit

sysdig

← Continuous Compliance (PCI, NIST, CIS, etc.) →

Source : [Kris Nova, Fixing the Kubernetes clusterfuck @FOSDEM]

Pourquoi ?

OWASP TOP 10 – 2013	OWASP TOP 10 – 2017
A1 – Injection	A1 – Injection
A2 – Broken Authentication and Session Management	A2 – Broken Authentication
A3 – Cross-Site Scripting (XSS)	A3 – Sensitive Data Exposure
A4 – Insecure Direct Object References **[Merged + A7]**	A4 – XML External Entities (XXE) **[NEW]**
A5 – Security Misconfiguration	A5 – Broken Access Control **[MERGED]**
A6 – Sensitive Data Exposure	A6 – Security Misconfiguration
A7 – Missing Function Level Access Control **[Merged + A4]**	A7 – Cross-Site Scripting (XSS)
A8 – Cross-Site Request Forgery (CSRF)	A8 – Insecure Deserialization **[NEW, COMMUNITY]**
A9 – Using Components with Known Vulnerabilities	A9 – Using Components with Known Vulnerabilities
A10 – Unvalidated Redirects and Forwards	A10 – Insufficient Logging & Monitoring **[NEW, COMMUNITY]**

Source: https://www.owasp.org/images/7/72/OWASP_Top_10-2017_%28en%29.pdf.pdf

Source : OWASP Top 10

Still alive

pry - Ben Bidmead and Guillaume Bonnet liked

HΔKLUKΞ
@hakluke

HTML injection is "'>alive and well

5:00 AM · Sep 9, 2020 · Twitter Web App

3 Retweets **106** Likes

HΔKLUKΞ @hakluke · 7h
Replying to @hakluke
jks... unicode
19

KUNDU IV @debangshu_kundu · 6h
Replying to @hakluke
Thank you for your submission however this issue is considered to be a P5 (Informational) finding as per XYZ's Vulnerability Rating Taxonomy, and therefore typically does not qualify for a reward.
5 19

Rudra16 @rudra16t · 6h
We are looking forward for more submission from you. Happy Hacking👍
6

Adil Burak @adilburaksen · 4h
Replying to @hakluke
If it's use with XSS bypass then useful. Otherwise it's not effective vuln.

Source : https://twitter.com/hakluke/

Gendarmerie nationale

" L'entrée en vigueur du RGPD modifie la posture des acteurs (des traitements) qui doivent tenir compte des impératifs de sécurité dès la conception d'un produit ainsi que son cycle de vie. Le label « by design » devient un label de qualité qui constituera un atout commercial. "

2022

- 90% des développements logiciels se déclaront DevSecOps (+40% 2019)
- 25% des développements IT selon DevOps (+10% 2019)

Source : Gartner/Techwire

Risque humain ?

ars TECHNICA

BIZ & IT TECH SCIENCE POLICY CARS GAMING & CULTURE STO

ELON SPEAKS —

Russian tourist offered employee $1 million to cripple Tesla with malware

"This was a serious attack," Elon Musk says.

DAN GOODIN - 8/28/2020, 4:12 AM

Tesla

Enlarge

Source : Ars Technica

Snyk TL;DR

TL;DR - The state of open source security 2019 report, at a glance

Open source adoption

- Growth in indexed packages, 2017 to 2018
  - Maven Central - 102%
  - PyPI - 40%
  - npm - 37%
  - NuGet - 26%
  - RubyGems - 5.6%
- npm reported 304 billion downloads for 2018
- 78% of vulnerabilities are found in indirect dependencies

Known vulnerabilities

- 88% growth in application vulnerabilities over two years
- In 2018, vulnerabilities for npm grew by 47%. Maven Central and PHP Packagist disclosures grew by 27% and 56% respectively
- In 2018, we tracked over 4 times more vulnerabilities found in RHEL, Debian and Ubuntu as compared to 2017

Known vulnerabilities in docker images

- Each of the top ten most popular default docker images contains at least 30 vulnerable system libraries
- 44% of scanned docker images can fix known vulnerabilities by updating their base image tag

Vulnerability identification

- 37% of open source developers don't implement any sort of security testing during CI and 54% of developers don't do any docker image security testings
- The median time from when a vulnerability was added to an open source package until it was fixed was over 2 years

Who's responsible for open source security?

- 81% of users feel developers are responsible for open source security
- 68% of users feel that developers should own the security responsibility of their docker container images
- Only three in ten open source maintainers consider themselves to have high security knowledge

Snyk stats

- In the second half of 2018 alone, Snyk opened more than 70,000 Pull Requests for its users to remediate vulnerabilities in their projects
- CVE/NVD and public vulnerability databases miss many vulnerabilities, only accounting for 60% of the vulnerabilities Snyk tracks
- In 2018 alone, 500 vulnerabilities were disclosed by Snyk's proprietary dedicated research team

4

Source : [The state of open source security – 2019]

Pour aller plus loin

- Sophia Security Camp 2019
- ANSSI Sécurité Agile (Atelier d'analyse de risque)

Analogie

« Nul n’est censé ignorer la loi »

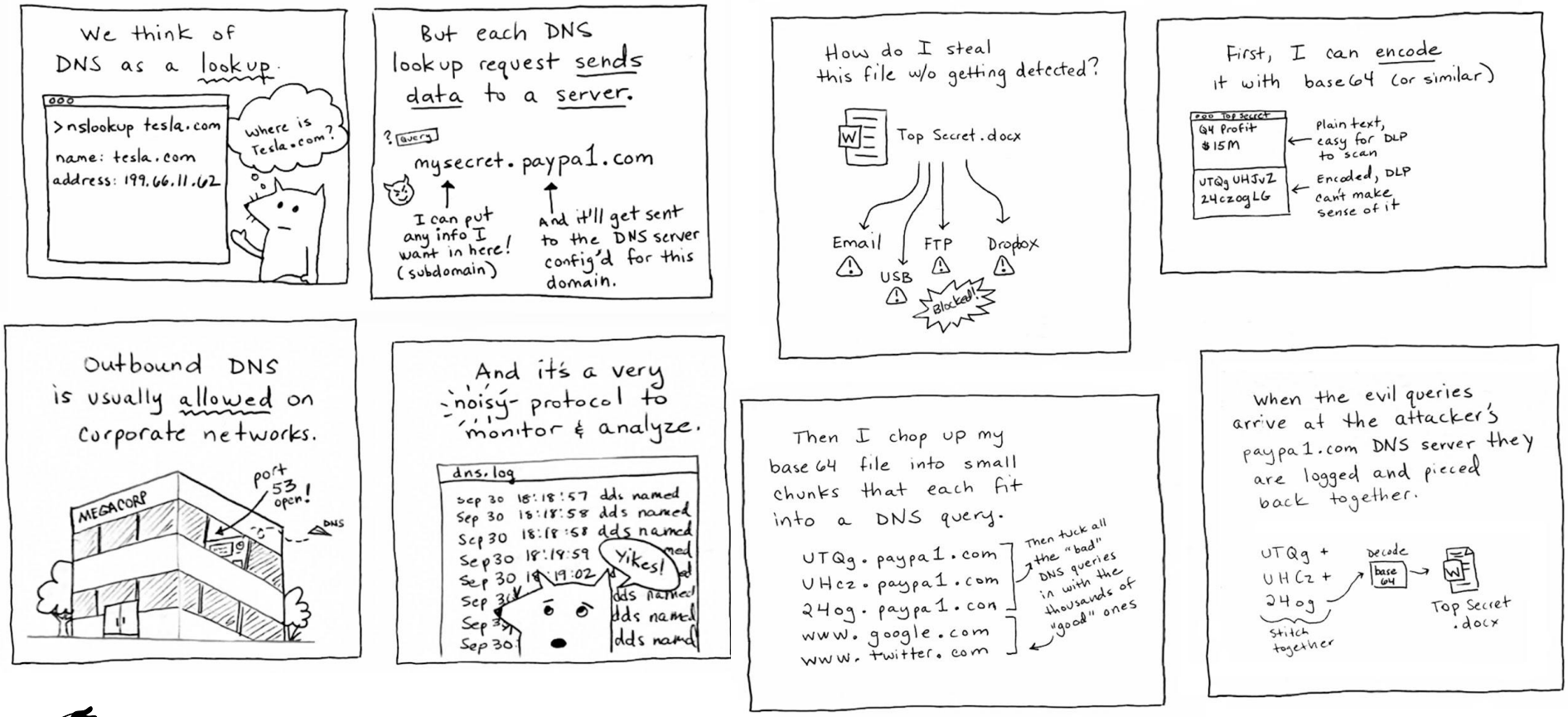
Ma devise

« Nul développeur n’est censé ignorer la sécurité »

Merci pour votre attention !

Avez-vous des questions ?

PS: Oui, j'essayerais 😅
#LaQuestionElleEstViteRépondue



Source : [Exfiltration DNS @Rob Sobers]

Maturité des équipes

Business Unit	Awareness and Training	Compliance and IT Audit	Emerging IT/Threats	Incident Response (IR)	Operations and Support	SDLC	PMO
1	2	3	2	1	2	2	3
2	3	2	3	2	3	2	2
3	2	3	2	1	2	1	3
4	3	3	2	2	3	3	3
5	2	2	3	1	1	2	1
6	2	3	2	1	1	2	2
7	3	2	3	2	3	2	3
8	3	3	3	3	3	3	3

Pas de MEP / Failure Fridays

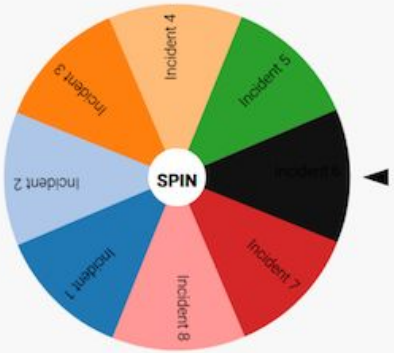
https://dastergon.gr/wheel-of-misfortune/

Wheel of Misfortune

A role-playing game for incident management training

Inspired by the Site Reliability Engineering book

Instructions



Incident 6

You've received alerts of high HTTP 5xx error rate...

Timing controls

Lap Clear

00:02:60

Pavlos Ratis | 2019

Source : [PagerDuty, 121, 200 tickets opened, 3 full AZ failures]

OVHcloud Datacenters