



#cloudest2021

@dadideo



1



# La sécurité dès la conception du projet

David Aparicio | 22 Octobre 2021 | 14h00 | Cloud Est (Room 2)



---

@dadideo

# David Aparicio

15/ DD INSA de Lyon / UNICAMP (Brésil)

Facebook Open Academy / MIT AppInventor

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

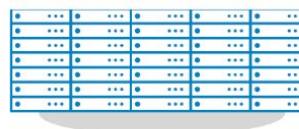
19/ Data(Sec)Ops @ OVHcloud (Lyon, 3 ans)



# OVHcloud: un leader européen

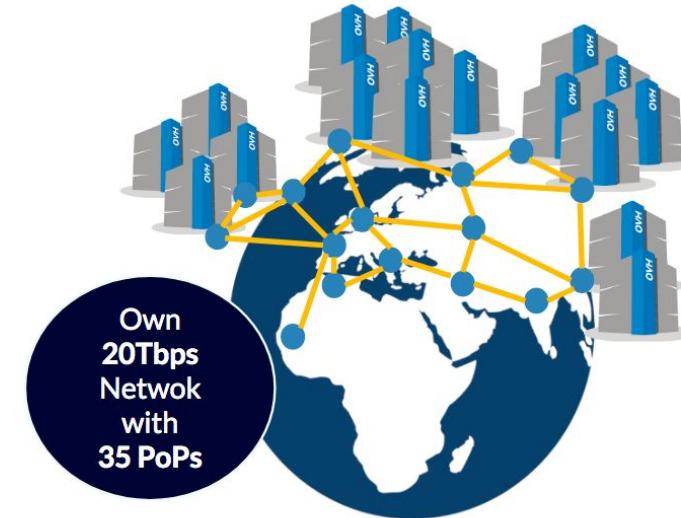
200k Private cloud

VMs running

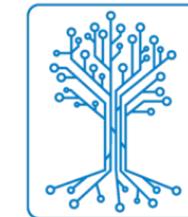


Hosting capacity :  
1.3M Physical  
Servers

360k  
Servers already  
deployed



> 1.3M Customers in 138 Countries



GAIA-X



# 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	T2 >20e
Virtualization	T3 >80e
Storage	T4 >300e
Database	T5 >600e
Bigdata	T6 >1200e
HCI	12KVA /32KVA
AI	
VDI	Cloud Game
Network	

**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	K8S, IA IaaS
Baremetal	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)
- Storage, Network, Databases

**Storage**

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

**AI**

- ElementAI, HuggingFace, Deepomatic, Systran, EarthCube

**Bigdata / Analytics / ML**

- Cloudera over S3, Dataku, Saage, Tableau,

**Hybrid Cloud**

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

**Secured Cloud**

- GOV, FinTech, Retail, HealthCare

# 16 au 18 Novembre 2021

# OVHcloud Ecosystem Experience



**Comment coopérer sur un cloud de confiance**

Rejoignez les leaders du cloud lors de notre événement annuel.

Du 16 au 18 novembre 2021

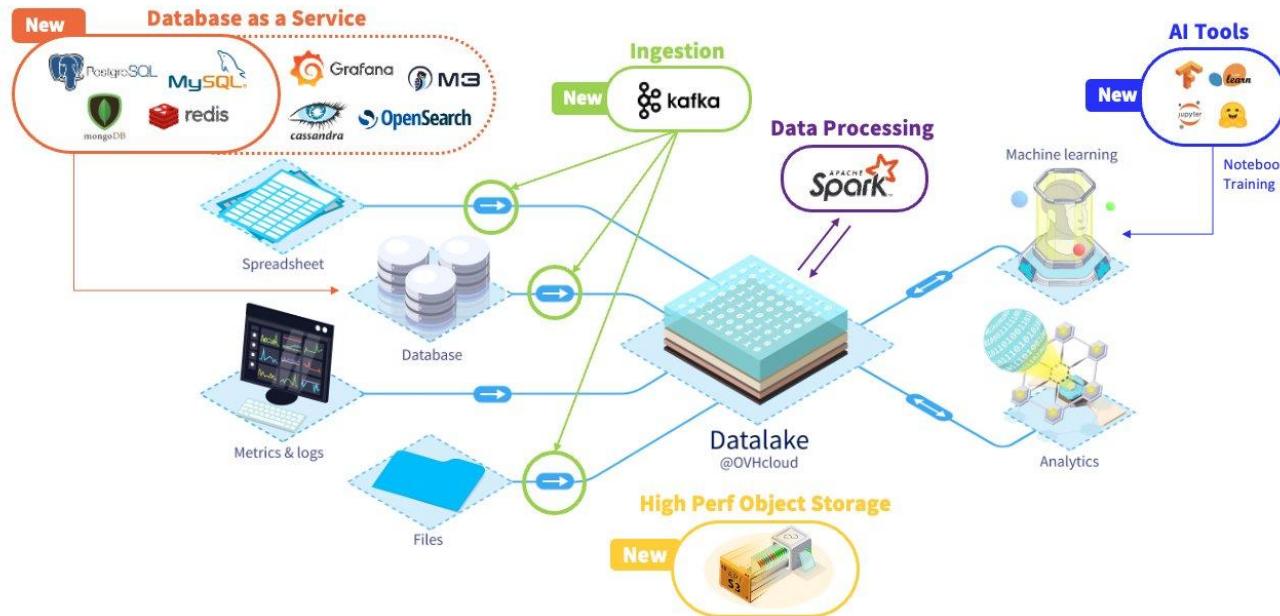
[Rejoignez les changemakers](#)

 EcoEx  
Ecosystem Experience

△ ▲ □

# Data @ OVHcloud

2021 : Improving our Public Cloud ecosystem for data projects

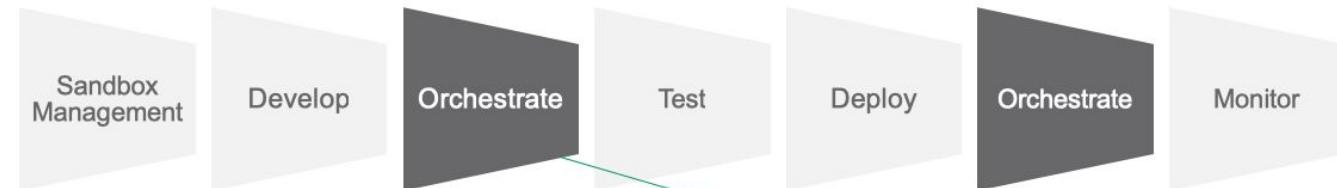


Bastien Verdebou

# DataOps @ GIS-DATA

- RéPLICATION des données
- Opérations Scaling (up/down), Maintenance (compactions, cleaning DB)
- PoC / Benchmarks / Performance tuning
- Industrialisation / Automatisation des procédures
- Mise en place de plate-forme de machine learning
- Urbanisation du Datalake
- Réalisation des Audits / Security assessment
- Migration des solutions
- Onboarding des projets
- RUN/BAU

## DataOps Process



There are thousands of tools, languages and vendors for Data





Mentimeter

# Présentation interactive

Gardez vos laptops/smartphones à portée 😊

Note: Étant en direct WorkAdventure, avec chacun, des connexions disparates, j'ai adapté mon support 😊





---

# Qui êtes-vous ?

Go to [www.menti.com](http://www.menti.com) and use the code 4296 4528



---

# La sécurité numérique et vous ?

Go to [www.menti.com](http://www.menti.com) and use the code 4296 4528



# Agenda

Introduction

Définitions

Piliers

Principes

Outils

Contexte

Conseils

Audits

Hackers

Remerciements

Conclusion



# Introduction



# Pourquoi ce talk ?

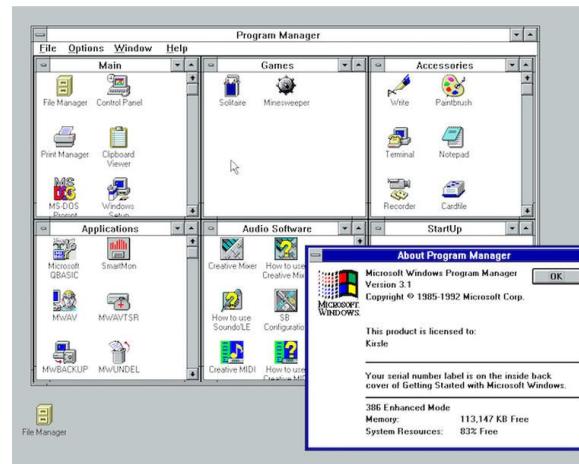
https://www.zdnet.com/article/a-23-year-old-windows-3-1-system-failure-crashed-paris-airport/

## 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)

### RECOMMENDED FOR YOU

How to drive speed, scale, and cost savings with data warehouse modernization

Live Event provided by Amazon Web Services

JOIN TODAY

### MORE FROM ZACK WHITTAKER



Security  
Online security 101: Tips for protecting your privacy from hackers and spies



Security  
US government's "do not buy" list shuts out Russia, China



Security  
New Spectre attack can remotely steal secrets, researchers say

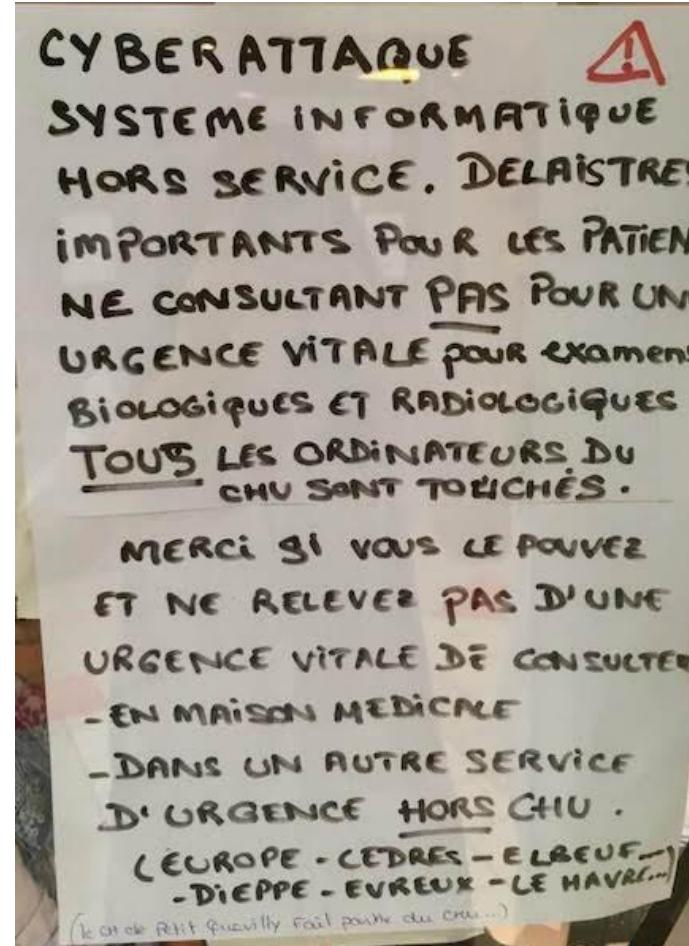


Security  
Flaw let researchers snoop on Swann smart security cameras

### NEWSLETTERS



# Pour éviter ceci



# Pour éviter cela

[Vos enjeux](#) [Services](#) [Secteurs d'activité](#) [Perspectives](#) [Investisseurs](#) [Nous](#)[Accueil](#) / [Médias](#) / [Communiqués de presse](#) / [Communiqué](#)

## Actualisation des informations relatives à la cyberattaque

[Partager](#)

Paris, 26 octobre 2020

Sopra Steria a annoncé le 21 octobre avoir détecté une cyberattaque la veille au soir. Le virus a été identifié : il s'agit d'une nouvelle version du ransomware Ryuk jusque-là inconnue des éditeurs d'antivirus et des agences de sécurité.

Les équipes d'investigation de Sopra Steria ont immédiatement fourni toutes les informations nécessaires aux autorités compétentes. La signature de cette nouvelle version du virus a donc pu être rapidement communiquée à tous les éditeurs d'antivirus pour mise à jour de leurs antivirus.

Il a par ailleurs été établi que la cyberattaque avait été lancée quelques jours seulement avant sa détection.

Les mesures de sécurité immédiatement mises en oeuvre ont ainsi permis de contenir la propagation du virus à une partie limitée des installations du Groupe et de préserver ses clients et ses partenaires.

A ce jour, et après des recherches approfondies, Sopra Steria n'a pas constaté de fuite de données ou de dommages causés aux systèmes d'information de ses clients.

Après analyse de l'attaque et élaboration du plan de remédiation, le redémarrage progressif et sécurisé du système d'information et des opérations du Groupe est engagé à compter de ce jour.

Le retour à une situation normale dans l'ensemble du Groupe prendra quelques semaines.



Ryuk, Sopra Steria [21/10/20]



---

## Que vous évoque "Sécurité (numérique) dès la conception" ?

Go to [www.menti.com](http://www.menti.com) and use the code 6525 6236



---

# En 2019, combien l'ANSSI a-t'elle enregistrée ?

Go to [www.menti.com](http://www.menti.com) and use the code 6525 6236

ANSSI : Agence nationale de la sécurité des systèmes d'information, créée en 2009  
chargée d'assister le Premier ministre dans l'exercice de ses responsabilités en matière de défense et de sécurité nationale



# Quelques chiffres



[Rapport ANSSI 2019](#)

Selon l'ANSSI

2296

Signalements en 2019

2018: 1869

2018: 16

2018: 14

9

Incidents majeurs

16

Opérations de cyberdéfense

2019: 370 incidents  
2018: 391 Incidents



---

# Quelques chiffres en Outre-Atlantique

Selon l'Institut Ponemon, en 2017

# 2,4 M\$

Ce qui coûte en moyenne à  
une entreprise, pour une  
attaque de malware

Selon le département américain de  
la Défense

# x 17

le nombres d'intrusions dans  
les infrastructures  
américaines cruciales en 3 ans



# Définitions





# Sécurité dès la conception

Dans le **domaine du génie logiciel**, le terme "Secure by design" (SBD) signifie que le produit a été conçu dès le départ pour être sûr [...] Dans cette approche, la **sécurité** est une **partie intégrante** au système, et commence par une conception d'architecture **robuste** [...] Tactiques de sécurité **bien connues** et des **modèles définis** comme des techniques **réutilisables** [...] Respecter les exigences nécessaires en matière d'authentification, d'autorisation, de confidentialité, d'intégrité des données, de respect de la vie privée, de responsabilité, de disponibilité, de sécurité et de non-répudiation, même lorsque le système est attaqué [...] il est non seulement important de concevoir une architecture de **sécurité robuste (prévue)**, mais il est également nécessaire de **préserver** l'architecture (mise en œuvre) pendant l'**évolution du logiciel** [...] Prendre soin de minimiser l'impact **en prévision** des vulnérabilités de sécurité

[Security By Design \[en anglais\]](#) / [Protection de la vie privée dès la conception](#)





# Sécurité dès la conception

Du domaine du **Génie Logiciel**

Souvent associé à **Privacy By Design**

Considérer la sécurité comme une **partie intégrante**

Conception d'architecture **robuste**

Résistant aux attaques **bien connues**

Utilisant des techniques **réutilisables**

Minimiser l'impact **en prévision** des vulnérabilités

Exigences dans de **multiples domaines** (auth., intégrité, confidentialité, etc..,)

Même lorsque le système est attaqué

**Préserver** l'architecture pendant l'**évolution du logiciel**

Mise en oeuvre durant tout le **cycle de vie**, jusqu'à la fin du support, et donc une date de **décommissionnement**





# Chronologie

## SdD-"Privacy By Design"

La première occurrence du mot "Sécurité dès la conception". Le terme est associé avec la notion "Conception respectueuse de la vie privée"

1995

1997

## Congrès EU

La première fois que la "Sécurité dès la Conception" est énoncée au sein du congrès de l'Union Européenne

2010

2016

## Mise en application du RGPD

Depuis le 25 Mai 2018. 6 grandes étapes sont identifiables: nomination d'DPO, recenser les traitements, définir les actions correctives, analyser le risque, établir des procédures internes et tenir une documentation à jour

2018

## Loi allemande

C'est la première fois qu'on retrouve le terme "Sécurité dès la conception" dans un texte de loi

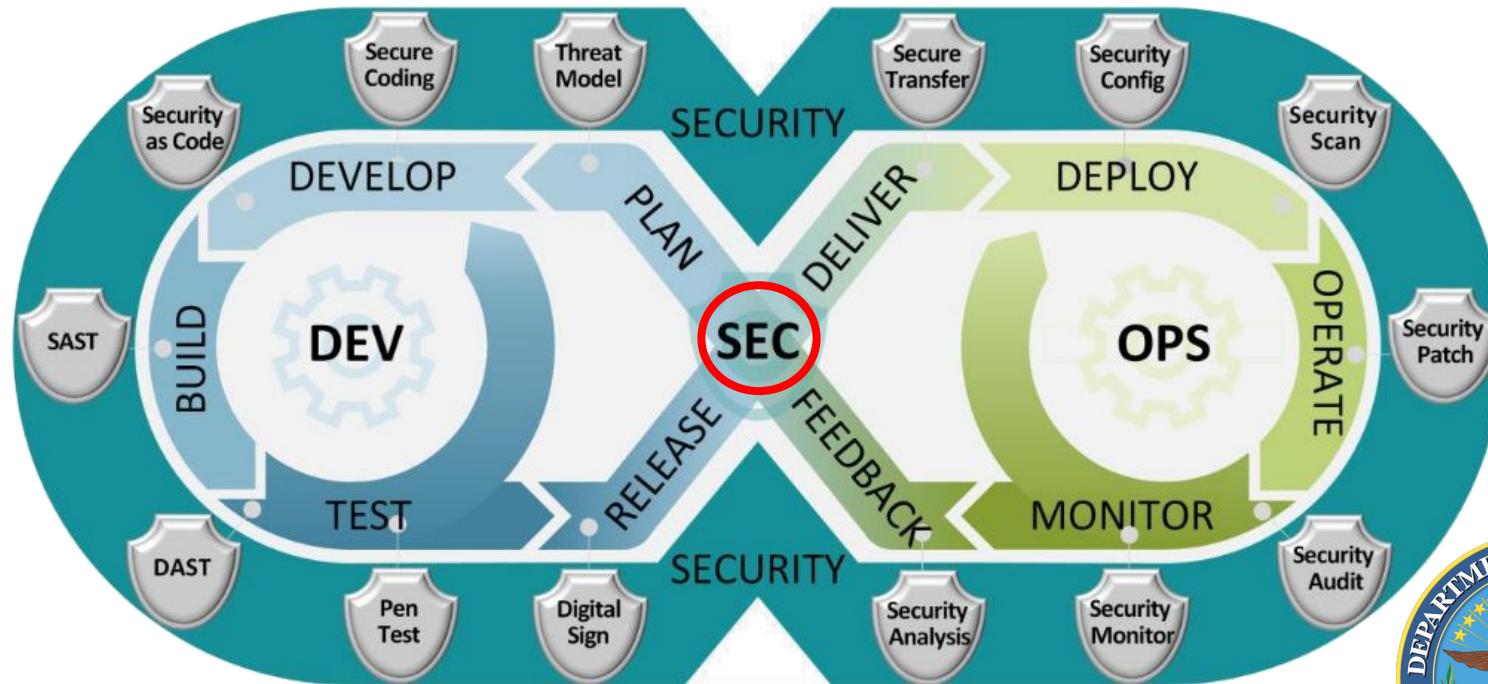
## Entrée en vigueur du 2016/679

Connue sur le nom de RGPD (Règlement Général sur la Protection des Données) [GDPR en anglais]. Elle impose un cadre légal sur le traitement des données personnelles, le consentement ainsi que leur cycle de vie

(Proposal COM/2012/0010)



# Shift-left Security



[dodcio.defense.gov](https://dodcio.defense.gov)





Pause pour les questions



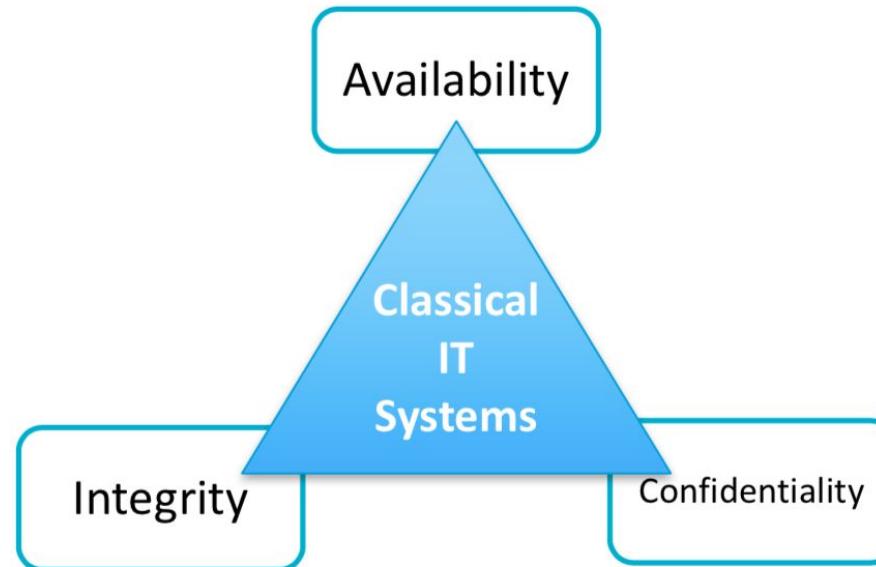


# Piliers

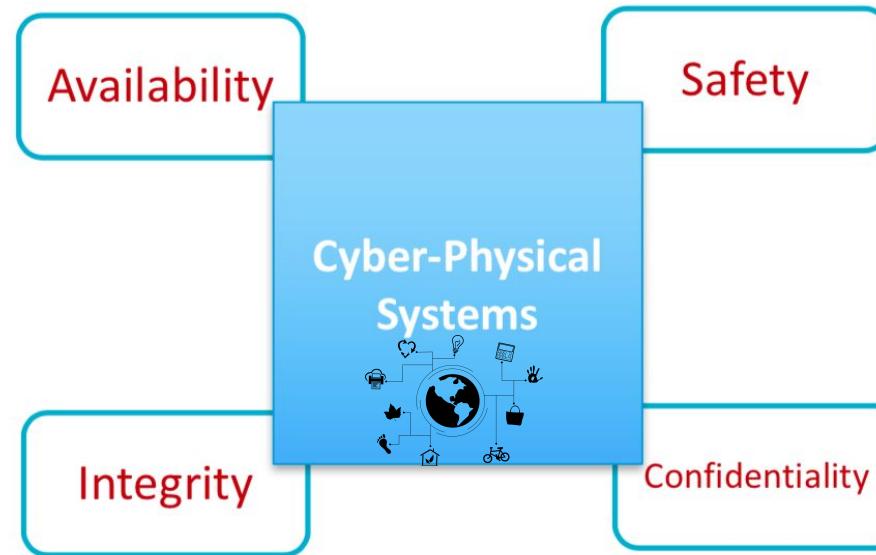
CIA+T / CAID  
DICT / DISP



# La sécurité de l'information



# Même dans le monde industriel



Cyber-menaces et cyber-préjudices : regards croisés

# Pour illustrer

## Y a-t-il un pilote à jour dans l'avion ?

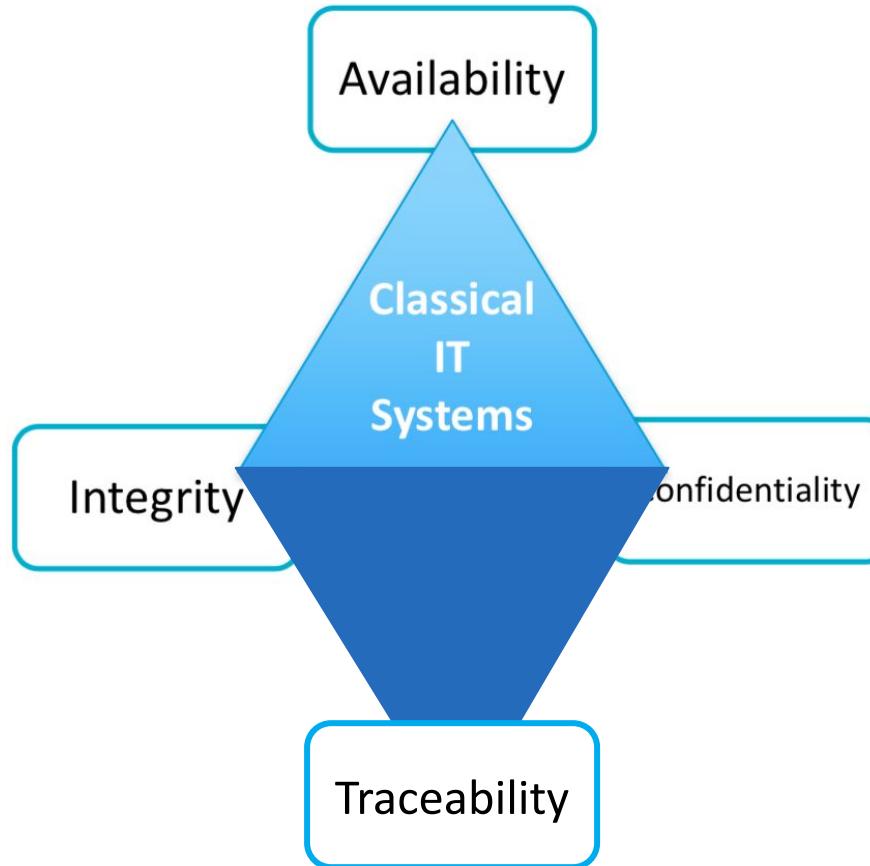
En 2015, les autorités états-unies de l'aviation alertaient les compagnies aériennes: le Boeing 787 Dreamliner devait être redémarré tous les 248 jours pour contourner un bogue pouvant entraîner une coupure de courant généralisée dont on peut imaginer les conséquences en vol. Cette fois, elles ont

annoncé qu'il faut éteindre et rallumer ces mêmes avions tous les 51 jours pour éviter des problèmes informatiques catastrophiques en raison d'une mémoire saturée de données sinon. Mesdames et Messieurs, veuillez regagner vos places et attacher vos ceintures de sécurité, nous allons bientôt rebouter!



Octobre 2020,  
Le Virus Informatique  
n°44 (papier/en ligne)

# DICT





---

# Confidentiality

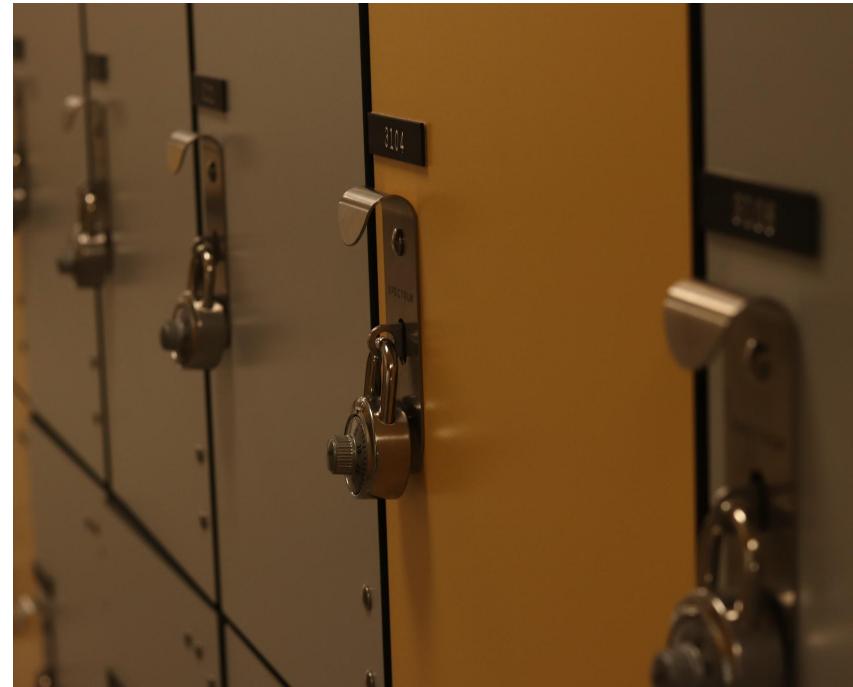
## O1 (Confidentialité)

La protection de la confidentialité consiste à préserver des informations secrètes. Tout ce qui attaque la capacité de chacun à préserver ce qu'il veut garder secret est une attaque contre la confidentialité.

**Exemples:**

Capture de trafic réseau

Propriété intellectuelle / Brevet





# Integrity

## 02 (Intégrité)

L'intégrité consiste à s'assurer que les informations n'ont pas été modifiées relativement à leur forme authentique. Les attaques contre l'intégrité sont celles qui essaient de modifier une information en vue d'une utilisation ultérieure.

### Exemples:

Comptes conformes au registre

Stocks conformes à l'inventaire

Modifications ou Corruption de la BDD ou du Excel

Formatage de disque dur





# Availability

## 03 (Disponibilité)

La disponibilité est un élément tout à fait critique du puzzle CIA. Comme on peut s'y attendre, les attaques contre la disponibilité sont celles qui font que la victime ne peut plus accéder à une ressource particulière.

### Exemples:

- Activer toutes les composants & services en HA
- Ne pas avoir de SPOF (Single Point of failure)
- Résister à des DDOS (Distributed Denial of Service)





# Traceability

## 04 (Traçabilité)

Parfois remplacé par Preuve, garantie que les accès et tentatives d'accès aux éléments considérés sont tracés et que ces traces sont conservées et exploitables.

La non-répudiation et l'imputation : aucun utilisateur ne doit pouvoir contester les opérations qu'il a réalisées dans le cadre de ses actions autorisées et aucun tiers ne doit pouvoir s'attribuer les actions d'un autre utilisateur (l'impersonification)

### Exemples:

Bastion

SIEM / Gestion de l'information et des événements de sécurité

Outils d'observabilité





# Illustration

## BDD

Forces d'une base de données

**Disponibilité:**

**Intégrité:**

Si les données ne sont pas intégrées, les actions des clients ou les décisions du métier pourraient être mauvaises

**Confidentialité:**

Les données, l'or noir du 21ème siècle, de plus, RGPD oblige

**Traçabilité:**

Comme il y a des données personnelles (PII), on doit avoir cette traçabilité de facto. Lignage de données/Maîtrise cycle de vie: création, stockage, partage, marquage, destruction de la donnée





---

# Illustration

## BDD

Faiblesses de la plate-forme après une revue DICT

**Disponibilité:**

Pas de HA, LDAP mono-machine, sans cache

**Intégrité:**

Service lancé en root, trop d'admins, pas de gestion de la configuration

**Confidentialité:**

Pas de garantie, pas de chiffrement, pas de TLS pour la communication

**Traçabilité:**

Pas de SIEM, accès direct depuis le bureau/bastion

Pas de logging externe, absence d'un outil de Data Lineage





Pause pour les questions





#cloudest2021

@dadideo



38



# Principles

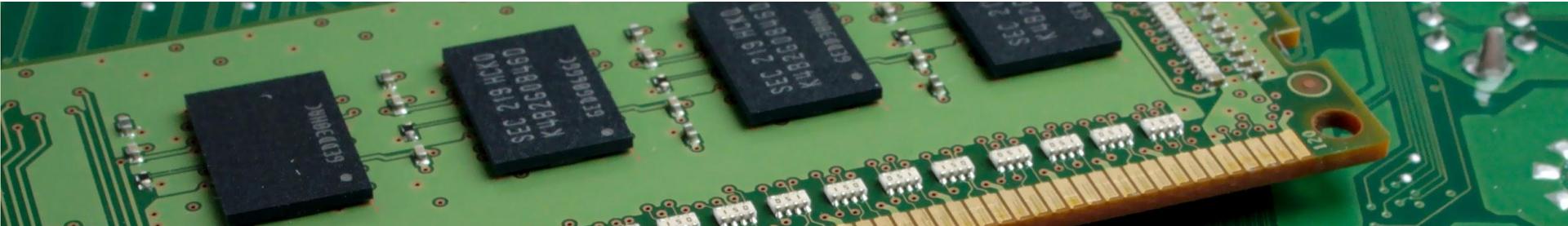




---

# Principe n°1 :

Minimiser la surface d'attaque

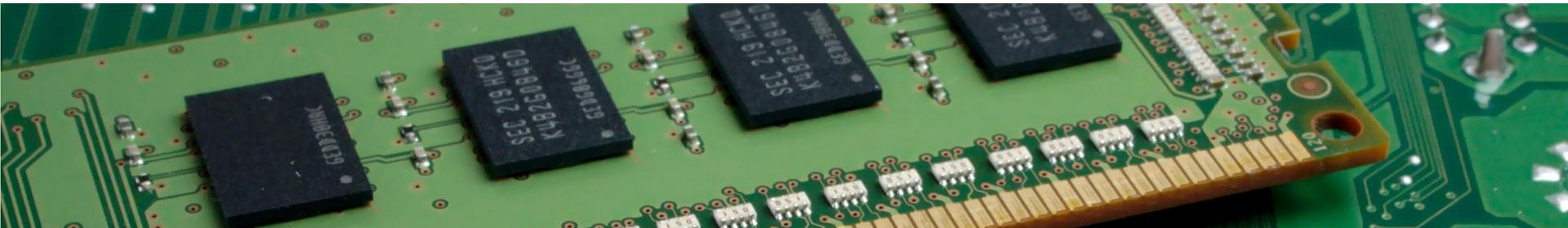




---

## Principe n°2 :

Le moindre privilège





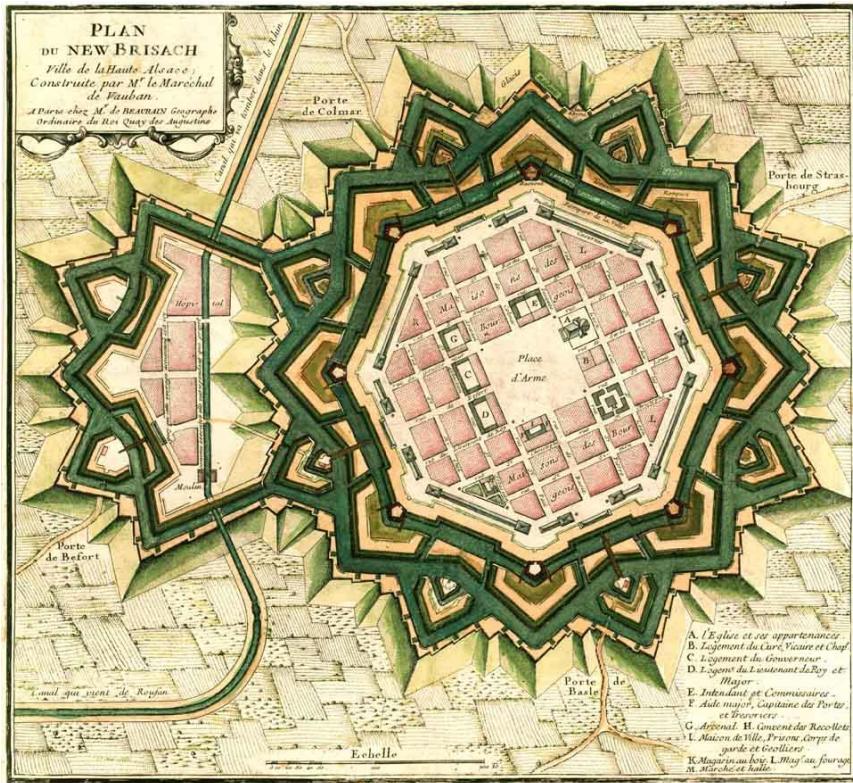
# Principe n°3 :

La défense en profondeur



The End of the Fortress Metaphor (EN)

Message à caractère informatique #21 - NAT Slipstreaming





Pause pour les questions



# 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:

```
#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;
}
```



[Deprecated code](#)



Pas copier-coller depuis StackOverFlow

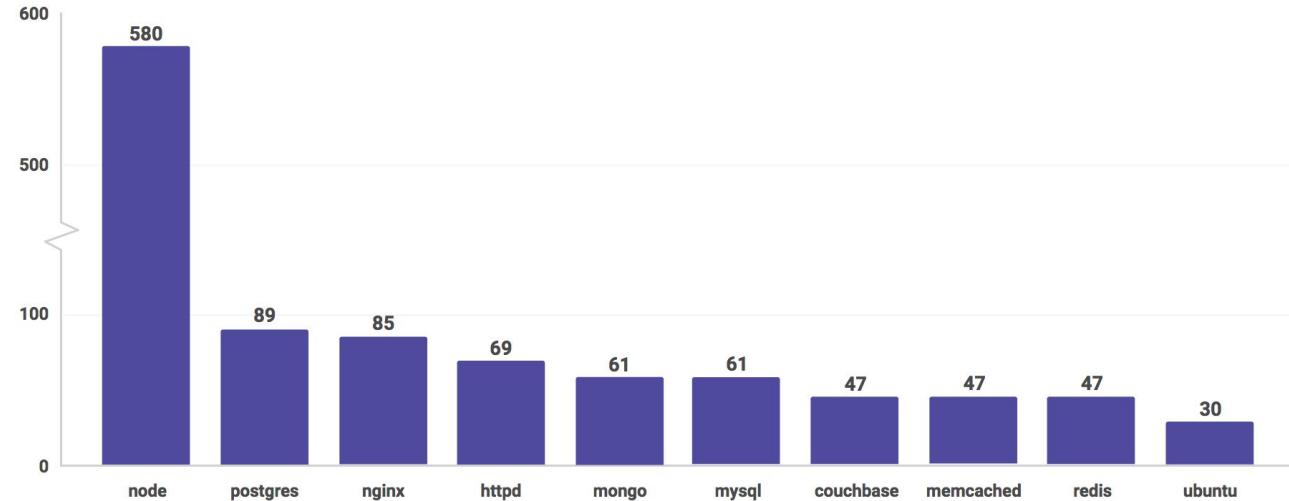
# 98% snippets sécu/crypto sont insecures



Fisher et al., 2017; Nadi et al., 2016; Das et al., 2014, Prevent cryptographic pitfalls by design

# Attention avec Docker

Number of OS vulnerabilities by docker image

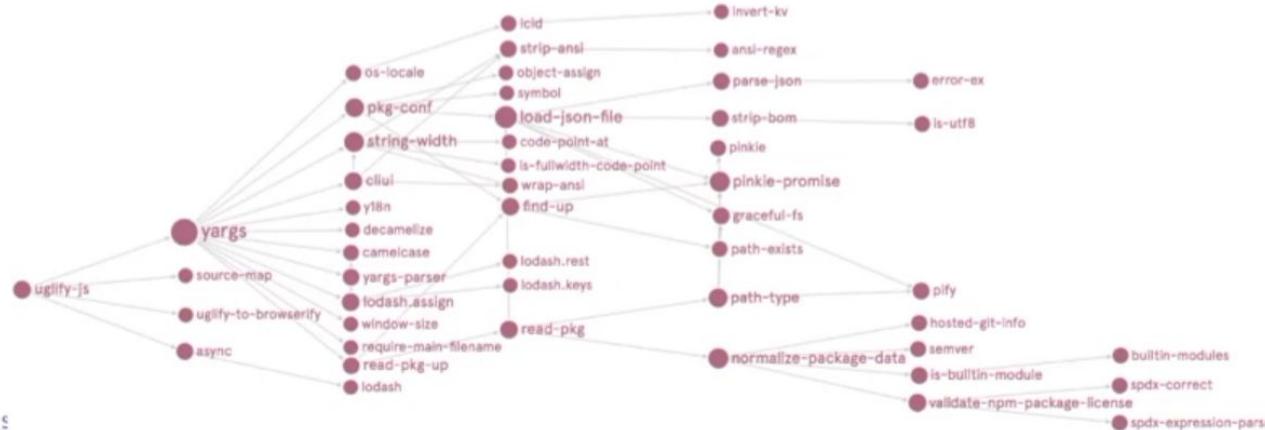


[The state of open source security – 2019](#)

# Attention avec vos dépendances

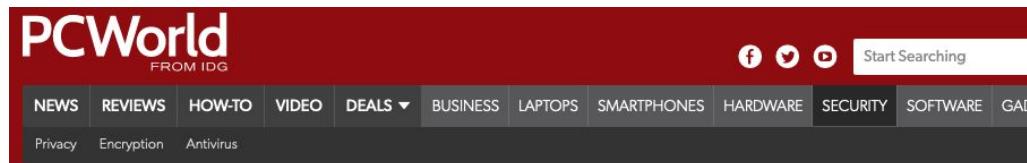
## Open Source Security report

- 78% of vulnerabilities are found in indirect dependencies



The state of open source security – 2019

# Attention avec vos dépendances



The image shows the header of the PCWorld website. The logo 'PCWorld' is at the top left, followed by 'FROM IDG'. To the right are social media icons for Facebook, Twitter, and YouTube, and a search bar with the placeholder 'Start Searching'. Below the header is a navigation bar with categories: NEWS, REVIEWS, HOW-TO, VIDEO, DEALS (with a dropdown arrow), BUSINESS, LAPTOPS, SMARTPHONES, HARDWARE, SECURITY, SOFTWARE, and GADG. A secondary navigation bar below it includes links for Privacy, Encryption, and 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



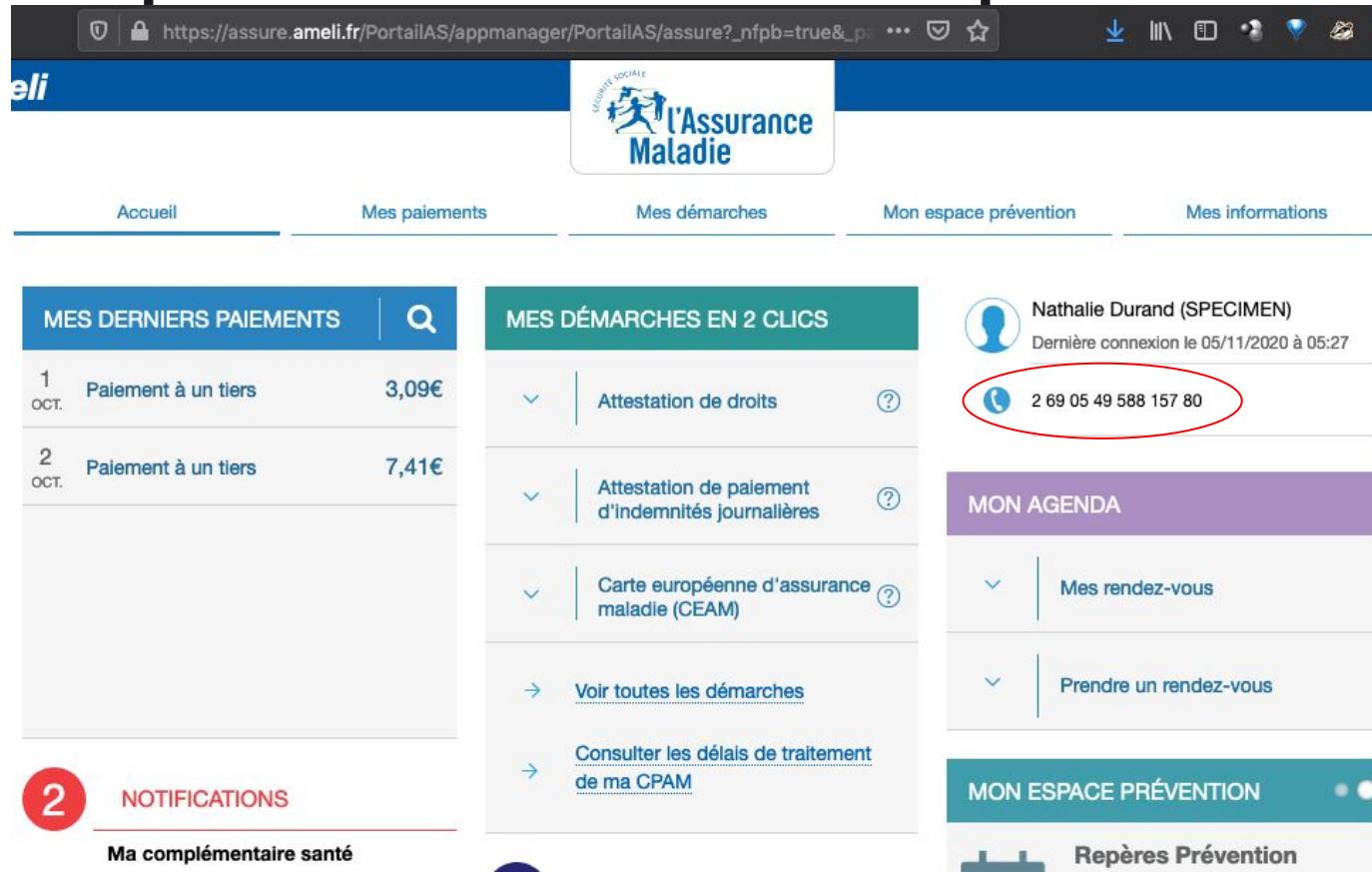
By [Lucian Constantin](#)

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



[PCWorld - Remote Code Execution Exploit \(Write-up\)](#)

# Ne pas afficher des données personnelles (PII)



The screenshot shows the Ameli.fr user interface. At the top, there's a navigation bar with links for Accueil, Mes paiements, Mes démarches, Mon espace prévention, and Mes informations. Below this is a main content area divided into several sections:

- MES DERNIERS PAIEMENTS**: Shows two recent payments: "Paiement à un tiers" on 1 OCT. for 3,09€ and another on 2 OCT. for 7,41€.
- MES DÉMARCHES EN 2 CLICS**: A list of quick actions:
  - Attestation de droits
  - Attestation de paiement d'indemnités journalières
  - Carte européenne d'assurance maladie (CEAM)
  - Voir toutes les démarches
  - Consulter les délais de traitement de ma CPAM
- MON AGENDA**: Options for viewing or scheduling appointments.
- MON ESPACE PRÉVENTION**: Options for prevention resources.

In the "MES DÉMARCHES EN 2 CLICS" section, the phone number 2 69 05 49 588 157 80 is circled in red to highlight it as a Personally Identifiable Information (PII) field.

Site d'Ameli.fr  
(numéro modifié pour illustrer)



CNIL - Donnée personnelle, Personally identifiable information (PII)

# Ne pas utiliser les configurations par défaut



mackeeper | [Blog](#)

Menu 

## BREAKING: Massive Breach of Mexican Voter Data

See the [interview with Chris Vickery](#) commenting on this breach.

Before going any further, let's make one thing very clear. I'm not the one who transmitted the data out of Mexico. Someone else will have to answer for that. However, eight days ago (April 14th), I did discover a publicly accessible database, hosted on an Amazon cloud server, containing these records. There was no password or authentication of any sort required. It was configured purely for public access. Why? I have no clue.

After reporting the situation to the US State Department, DHS, the Mexican Embassy in Washington, the Mexican Instituto Nacional Electoral (INE), and Amazon, the database was finally taken offline April 22nd, 2016.

Under Mexican law, these files are “strictly confidential” carrying a penalty of up to 12 years in prison for anyone extracting this data from the government for personal gain. We’re talking about names, home addresses, birthdates, a couple of national identification numbers, and a few other bits of info.



[Massive Breach of Mexican Voter Data](#)

# Ne pas utiliser les configurations par défaut



< Home > Blog > Report: Hotel Reservation Platform Leaves Millions of People Exposed in Massive Data Breach

## Report: Hotel Reservation Platform Leaves Millions of People Exposed in Massive Data Breach

 Mark Holden November 06, 2020

**Inside this Article ▾**

**Company:** Prestige Software, based in Spain.

**Severity:** High

**Size:** 24.4 GB, totaling 10,000,000+ exposed files

**Data Storage Format:** Misconfigured AWS S3 bucket

**Countries Affected:** Worldwide

Courtesy of our security team at [Website Planet](#), we can reveal that a hotel reservation platform has been exposing highly sensitive data from millions of hotel guests worldwide, dating as far back as 2013 and including credit card details for 100,000s of people.

Based in Madrid and Barcelona, Prestige Software sells a channel management platform called Cloud Hospitality to hotels that automates their availability on online booking websites like Expedia and Booking.com.

The company was storing years of credit card data from hotel guests and travel agents without any protection in place, putting millions of people at risk of fraud and online attacks.

### Customer Data Exposed

- **PII data:** Full names, email addresses, national ID numbers, and phone numbers of hotel guests

Prestige Software doesn't list that appeared to originate from including, but not limited to:

- Agoda
- Amadeus
- Booking.com
- Expedia
- Hotels.com
- Hotelbeds
- Omnibees
- Sabre
- and many others



[Hotel Reservation Platform Leaves Millions of People Exposed in Massive Data Breach](#)



# Pourquoi tout cela ?





---

## Pour résumer

- Diminuer surface d'attaque (scratch, distroless)
- Principe de moindre privilège !root
- Défense en profondeur (bastion, traceability, siem)
- Détection de connexion, MFA
- Pas de configuration par défaut (K8s, [MongoDB](#))
- Pas de secrets dans les Docker images ou les repositories Git (Vault, .gitignore)
- Pas de données sensibles dans les GUI
- Ne pas afficher de stacktrace (pas debug | Fail securely)
- Ni de version/nom de framework
- Vérifier les entrées/sorties des clients/noeuds (injection/XSS)
- Faire des backups régulièrement & déconnectées du réseau
- 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



Pause pour les questions





**C'est quand qu'tu vas m'mettre  
des paillettes dans ma vie  
David**

---



# Outils





#cloudest2021

@dadideo



57



# DevOps





#cloudest2021

@dadideo



58



# CI/CD

Pipeline Jobs 5



[https://twitter.com/k33g\\_org/](https://twitter.com/k33g_org/)



# Plan: Threat Model





# Bonnes pratiques ANSSI

Se documenter, se former

Lire les guides de l'ANSSI

Comparer les technologies, les langages de programmation

Effectuer l'analyse des risques

Identifier le modèle de l'attaquant pour ce produit en particulier

Préparer des spécifications / des ateliers

Participer à des conférences Sécurité

Choix du système hôte ([OS hardening](#))

Veille technologique ([Feedly/RSS](#))



ANSSI

Agence nationale de la sécurité des  
systèmes d'information



RECOMMANDATIONS RELATIVES À L'INTERCONNEXION D'UN SYSTÈME D'INFORMATION  
Réseaux

19/06/2020

architecture interconnexion Internet messagerie passerelle



RÈGLES DE PROGRAMMATION POUR LE DÉVELOPPEMENT D'APPLICATIONS SÉCURISÉES  
09/06/2020

application sécurisée bonne pratique développement sécurisé langage de  
règle



RECOMMANDATIONS DE SÉCURITÉ RELATIVES À TLS  
Cryptographie Réseaux

26/03/2020

chiffrement HTTPS TLS



RECOMMANDATIONS SUR LA SÉCURISATION DES SYSTÈMES DE CONTRÔLE D'ACCÈS PHYSIQUE  
ET DE VIDÉOPROTECTION



[Bonnes pratiques de sécurité numérique \(ANSSI\)](#)



# Dev: Secure Coding/SaC





# Linters

## Go

Un linter est un outil d'analyse statique de code source. Il sert à détecter : des erreurs (très utile sur des langages interprétés comme JavaScript qui n'ont pas de phase de compilation) ; des problèmes de syntaxe et de non-respect de style (tabulation vs espaces, indentation, etc.)

```
linters:  
  disable-all: true  
  enable:  
    - bodyclose  
    - deadcode  
    - depguard  
    - dogsled  
    - dupl  
    - errcheck  
    - funlen  
    - goconst  
    - gocritic  
    - gocyclo  
    - gofmt  
    - goimports  
    - golint  
    - gomnd  
    - goprintffuncname  
    - gosec  
    - gosimple  
    - govet  
    - ineffassign  
    - interfacer  
    - misspell  
    - nakedret  
    - rowerrcheck  
    - scopelint  
    - staticcheck  
# - ...
```

## STATIC LINTS WITH GOLANG-CI



Customize: linters list, values...

In few situations you can bypass the linters with nolint directive.

//nolint



"Common mistakes" en Go, Aurélie Vache  
(RDV des Speakers 2020)



# Linters Shell

Il permet d'avoir un code avec moins d'effets de bord  
Disponible dans (quasiment) tous les langages

```
$ shellcheckmyscript

Line 4:
if ! grep -q backup=true.* "~/.myconfig"
    ^-- SC2062: Quote the grep pattern so the
                  ^-- SC2088: Tilde does not

Line 6:
echo 'Backup not enabled in $HOME/.myconfig, exiting'
    ^-- SC2016: Expressions don't expand in single

Line 10:
if [[ $1 =~ "-v(erbose)??" ]]
    ^-- SC2076: Don't quote right-hand side of

Line 12:
verbose='printf "Copying %f\n"'
    ^-- SC2089: Quotes/backslashes will be treated

Line 16:
-iname *.tar.gz \
    ^-- SC2061: Quote the parameter to -iname so
                  ^-- SC2035: Use ./glob* or -- *glob* so name
```



[ShellCheck, finds bugs in your shell scripts](#)



#cloudest2021

@dadideo



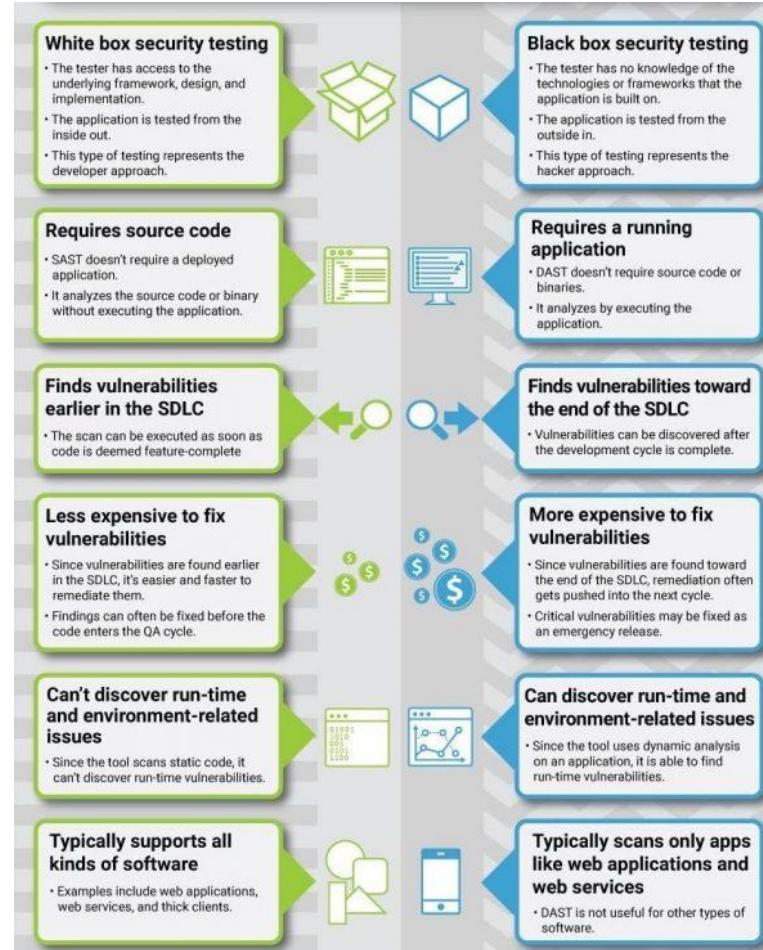
64



# Build: SAST / DAST / IAST



# SAST DAST IAST App Security Test





# GitGuardian

## Activity

Overview

122 Policy breaks

151 Monitored events

Monitored events and policy/breaks

Date	Author	Source	Policy	Status
Feb 10th 2020 11:12	Tom Dupont	prm-dev-team/tom_gordon	SendGrid Key Secret detection	RESOLVED
Feb 10th 2020 11:12	Michel Smith	prm-dev-team/flash_time	Slack Bot Token File extensions	TRIGGERED
Feb 10th 2020 11:12	Tom Dupont	prm-dev-team/tom_gordon	SendGrid Key Secret detection	RESOLVED
Feb 10th 2020 11:12	Michel Smith	prm-dev-team/flash_time	Slack Bot Token File extensions	IGNORED
Feb 10th 2020 11:12	Tom Dupont	prm-dev-team/tom_gordon	SendGrid Key Secret detection	RESOLVED
Feb 10th 2020 11:12	Michel Smith	prm-dev-team/flash_time	Slack Bot Token File extensions	TRIGGERED
Feb 10th 2020 11:12	Tom Dupont	prm-dev-team/tom_gordon	SendGrid Key Secret detection	RESOLVED
Feb 10th 2020 11:12	Michel Smith	prm-dev-team/flash_time	Slack Bot Token File extensions	TRIGGERED

## Up and running in a minute

Integrate natively with GitHub or use our API to integrate GitGuardian into your CI pipeline.

## Value delivered right away

Scan your existing code repositories for secrets left in your git history.

## Integrate with your tools

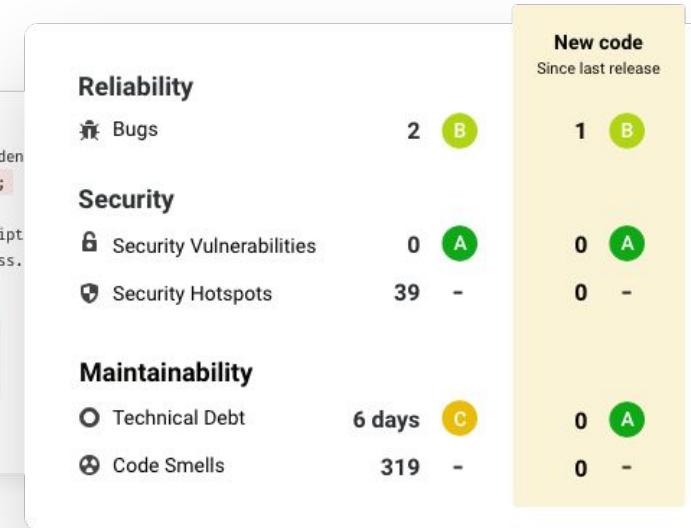
Integrate with most common ticketing and notification systems, as well as SSO providers.



Automated Secrets Detection for Application Security

# 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 }
```



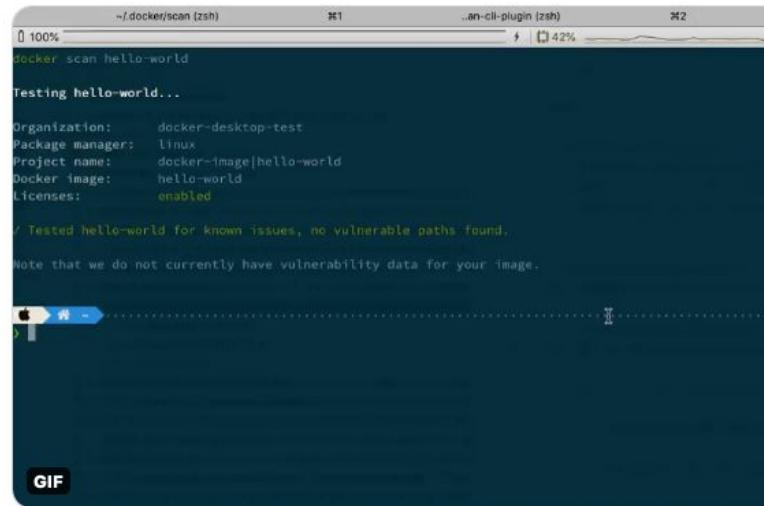
# Docker CLI



Guillaume 🐾  
@glours

Replying to @glours @silvin\_docker and 2 others

With a better Gif and a link to the documentation  
[docs.docker.com/engine/scan/](https://docs.docker.com/engine/scan/)



```
~/docker/scan (zsh) 11 ..an-cli-plugin (zsh) 12
0 100% docker scan hello-world

Testing hello-world...

Organization: docker-desktop-test
Package manager: linux
Project name: docker-image|hello-world
Docker image: hello-world
Licenses: enabled

/ Tested hello-world for known issues, no vulnerable paths found.

Note that we do not currently have vulnerability data for your image.

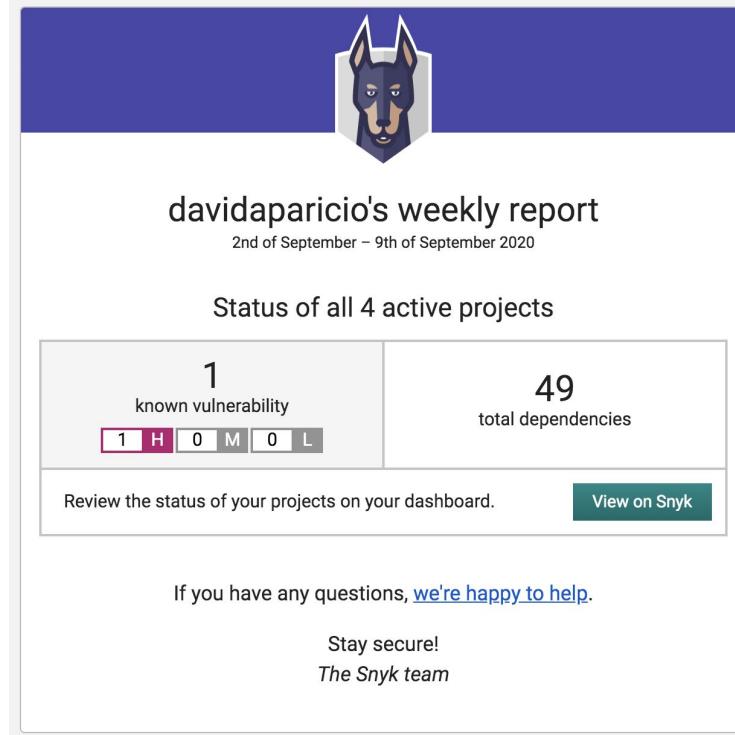
GIF
```

12:11 PM · Sep 2, 2020 · TweetDeck



Vulnerability scanning - Docker Documentation

# Snyk



The image shows a screenshot of a Snyk weekly report dashboard. At the top, there's a purple header featuring the Snyk logo (a stylized dog head) and the text "davidaparicio's weekly report" followed by the date range "2nd of September – 9th of September 2020". Below the header, a section titled "Status of all 4 active projects" displays key metrics: "1 known vulnerability" (with severity levels 1 H, 0 M, 0 L) and "49 total dependencies". A call-to-action button "View on Snyk" is located next to this information. Further down, a message encourages users to "Review the status of your projects on your dashboard." At the bottom, there's a note: "If you have any questions, [we're happy to help.](#)" followed by "Stay secure!" and "The Snyk team".





# npm-audit

## Javascript

Auditer les vulnérabilités connues des librairies et des dépendances associées

High	Arbitrary File Overwrite
Package	tar
Patched in	>=4.4.2
Dependency of	libnpm
Path	libnpm > npm-lifecycle > node-gyp > tar
More info	<a href="https://npmjs.com/advisories/803">https://npmjs.com/advisories/803</a>
High	Arbitrary File Overwrite
Package	tar
Patched in	>=4.4.2
Dependency of	npm-lifecycle
Path	npm-lifecycle > node-gyp > tar
More info	<a href="https://npmjs.com/advisories/803">https://npmjs.com/advisories/803</a>

```
Found 19 vulnerabilities (8 moderate, 11 high) in 11360 scanned packages
run `npm audit fix` to fix 4 of them.
12 vulnerabilities require semver-major dependency updates.
3 vulnerabilities require manual review. See the full report for details.
```



# 19/10/20

→ C ⌂ 🔒 https://securite.developpez.com/actu/309772/Quatre-packages-npm-trouves-en-train-d-ouvrir-des-shells-sur-des-systemes

## Quatre packages npm trouvés en train d'ouvrir des shells sur des systèmes Linux et Windows.

Tout ordinateur avec l'un de ces packages installés « doit être considéré comme totalement compromis »

Le 19 octobre 2020 à 12:27, par Stan Adkens

6 commentaires



364 PARTAGES



L'équipe de sécurité de npm a supprimé la semaine dernière quatre packages hébergés sur son dépôt, découverts en train d'ouvrir des shells afin d'établir une connexion à des serveurs distants pour exfiltrer les données des utilisateurs à partir des systèmes Linux et Windows infectés. Selon l'équipe de sécurité, chaque bibliothèque a été téléchargée des centaines de fois depuis son chargement sur le portail npm.

Les noms des quatre packages npm sont : plutov-slack-client, nodetest199, nodetest1010 et npmpubman. Les packages ont été mis en ligne sur le portail npm en mai 2018 (en ce qui concerne le premier) et en septembre de la même année (pour le reste). Jeudi dernier, le personnel du npm a retiré les quatre paquets JavaScript du portail npm parce qu'ils contenaient du code malveillant.



npm est le plus grand dépôt de packages pour tous les langages de programmation. L'équipe de sécurité de npm scanne régulièrement sa collection de bibliothèques JavaScript, considérée comme le plus important dépôt. Bien que les paquets malveillants soient régulièrement supprimés, la suppression de la semaine dernière est la troisième grande mesure de répression de ces trois derniers mois.

Selon les avis publiés par l'équipe de sécurité de npm, les quatre bibliothèques JavaScript ont ouvert des shells sur les ordinateurs des développeurs qui ont importé ces packages dans leurs projets. Les shells permettaient aux acteurs de la



### 4 packages npm ouvrent des shells [Linux/Windows]

# DAST (Gitlab)

Language (package managers) / framework	Scan tool
.NET Core	<a href="#">Security Code Scan</a>
C/C++	<a href="#">Flawfinder</a>
Go	<a href="#">Gosec</a>
Helm Charts	<a href="#">Kubesec</a>
Java ( <a href="#">Ant</a> , <a href="#">Gradle</a> , <a href="#">Maven</a> , <a href="#">SBT</a> )	<a href="#">SpotBugs</a> with <a href="#">find-sec-bugs</a>
Java / Kotlin (Android)	<a href="#">MobSF (beta)</a>
JavaScript	<a href="#">ESLint security plugin</a>
Kubernetes manifests	<a href="#">Kubesec</a>
Node.js	<a href="#">NodeJsScan</a>
PHP	<a href="#">phpcs-security-audit</a>
Python ( <a href="#">pip</a> )	<a href="#">bandit</a>

## Available rules

- G101: Look for hard coded credentials
- G102: Bind to all interfaces
- G103: Audit the use of unsafe block
- G104: Audit errors not checked
- G106: Audit the use of ssh.InsecureIgnoreHostKey
- G107: Url provided to HTTP request as taint input
- G108: Profiling endpoint automatically exposed on /debug/pprof
- G109: Potential Integer overflow made by strconv.Atoi result conversion to int16/32
- G110: Potential DoS vulnerability via decompression bomb
- G201: SQL query construction using format string
- G202: SQL query construction using string concatenation
- G203: Use of unescaped data in HTML templates
- G204: Audit use of command execution
- G301: Poor file permissions used when creating a directory
- G302: Poor file permissions used with chmod
- G303: Creating tempfile using a predictable path
- G304: File path provided as taint input
- G305: File traversal when extracting zip/tar archive
- G306: Poor file permissions used when writing to a new file
- G307: Deferring a method which returns an error
- G401: Detect the usage of DES, RC4, MD5 or SHA1
- G402: Look for bad TLS connection settings
- G403: Ensure minimum RSA key length of 2048 bits
- G404: Insecure random number source (rand)
- G501: Import blocklist: crypto/md5
- G502: Import blocklist: crypto/des
- G503: Import blocklist: crypto/rc4
- G504: Import blocklist: net/http/cgi
- G505: Import blocklist: crypto/sha1
- G601: Implicit memory aliasing of items from a range statement

## Retired rules

- G105: Audit the use of math/big.Int.Exp - CVE is fixed



# 42Crunch

## Scanner d'API

Assurer la sécurité des API au rythme du Business  
et ne JAMAIS laisser des API non sécurisées atteindre la PROD

Vérifie la consistance de votre API par rapport au contrat  
d'interface

Utilise la spécification OpenAPI / Swagger pour identifier les  
faiblesses de votre API



Protection contre le Top 10 de la  
sécurité de l'API de l'OWASP

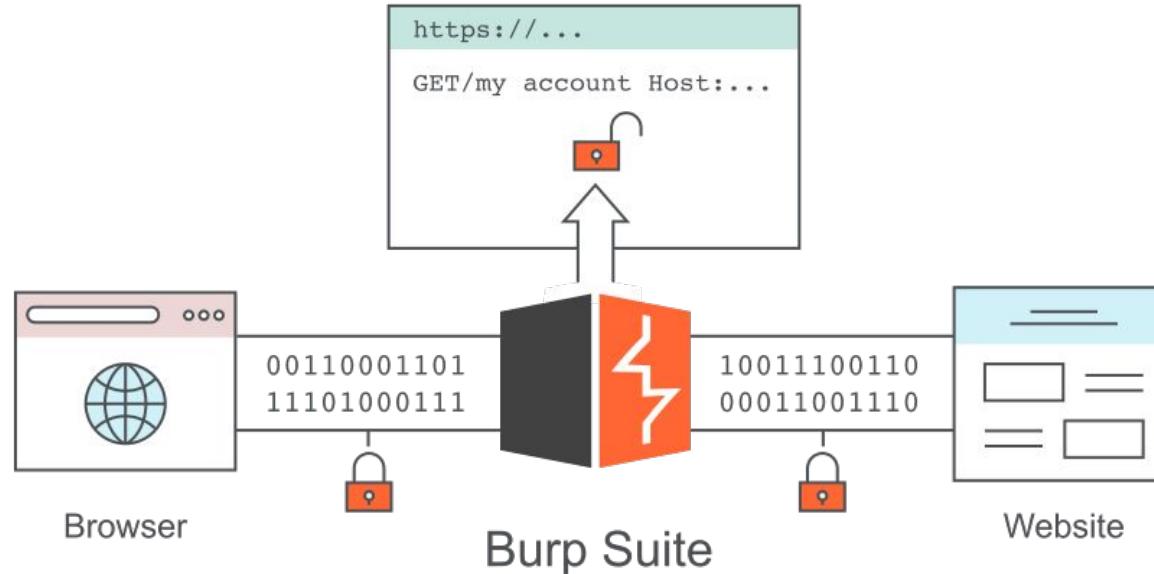
The screenshot displays the 42Crunch Platform interface. At the top, a browser window shows the URL <https://platform.42crunch.com/apis/4a0ff95-1d9a-4d97-fe4d7cc474be/api-summary>. The main dashboard features a "Security Audit" card with an audit score of 84 / 100 and a "Conformance Scan" card showing 41 issues. To the right, a "Protection" section indicates an "ACTIVE" status for the API firewall. Below the dashboard, a Visual Studio Code editor window is open, displaying an OpenAPI JSON file (PixiBasic-v1.0.json) and a "API Security Audit" panel. The audit panel highlights a critical finding: "The security section of the operation 'post' contains an empty array". It also lists other findings under "Security (18/30)" and "Data validation (25/70)". The bottom of the screen shows standard VS Code navigation and status bars.



# Test: PenTest



# Proxy



Security Bug Hunting with Proxies (Black Box) : Burp Suite, OWASP ZAP, mitmproxy, charles

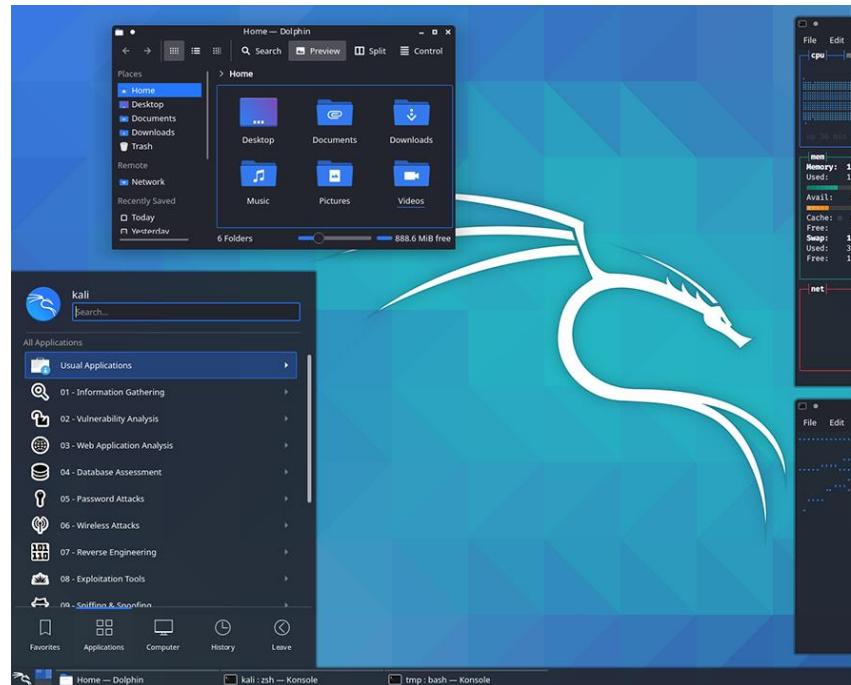


# Kali Linux / Parrot OS

## Boîte à outils

Les tests d'intrusion sont un moyen de trouver et de colmater des brèches. Objectif: Simuler des attaques pour tester la robustesse de la plate-forme

- Nmap
- Metasploit
- Wireshark
- John The Ripper
- Hashcat
- Hydra
- Burp Suite
- Zed Attack Proxy (ZAP)
- sqlmap
- aircrack-ng



11 outils pour s'initier au pentest



# Hackers as a Service





# Release: Digital Signature

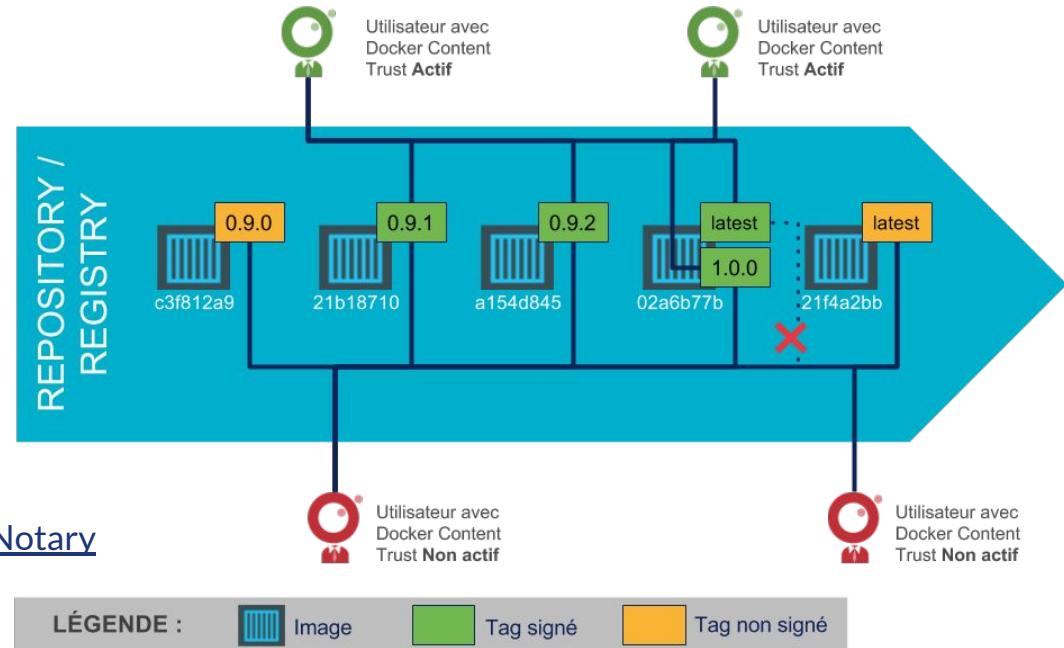




# Docker Notary

## Ready for PROD

Signer pour certifier et être avoir la garantie sur la provenance (non-altération)



[Documentation Docker Notary \[EN\]](#)  
[La signature d'images Docker sur une Registry avec Notary](#)



#cloudest2021

@dadideo



80



# Deliver: Secure Transfer





# JFrog Artifactory Repository

Signer pour certifier, être avoir la garantie sur la provenance (non-altération), archiver et faciliter les rollbacks

The screenshot shows the JFrog Artifactory interface. The left sidebar has icons for Cloud, Artifactory, Docker, Bintray, and Remote Cache. The main area is titled "Artifact Repository Browser". On the left, there's a tree view showing a "docker" folder, which contains a "docker-local" folder. Inside "docker-local", there's a "hello-world" folder with an "uploads" subfolder containing a file named "v1.0". Other items listed include "bintray-docker-remote-cache" and "docker-remote-cache". On the right, there's a detailed view for the "docker" repository. It shows the "General" tab with the following information:

Info	Value
Name:	docker
Package Type:	Docker
Repository Path:	docker/
Repository Layout:	simple-default

Below this, there's a section for "Included Repositories" listing "docker-local", "bintray-docker-r...", and "docker-remote". There are also "Set Me Up" and "Deploy" buttons at the top right.



# Deploy: Security Conf/Scan





# Argo CI + Vault

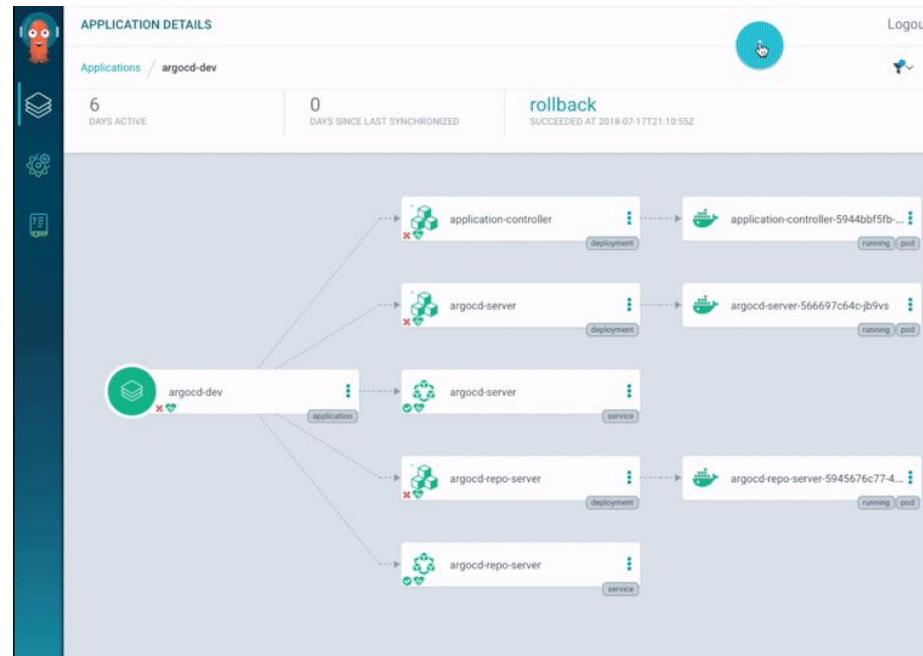
## Keep immutable

Les définitions, configurations et environnements des applications doivent être déclaratifs et contrôlés par version. Le déploiement et la gestion du cycle de vie des applications doivent être automatisés, contrôlables et faciles à comprendre

-> Maintenir un système iso aux specs



[Why Argo CD? \[EN\]](#)





# Operate: Secu. Patch/Audit





# Ansible / Chef / Puppet

## Patch & Reboot

Maintenir un système à jour en installant les patchs de sécurité

- Linux
- Windows
- Mac OS
- iOS
- Android
- /e/
- etc...



Playbook: apply patches & perform a reboot if required

```
---
```

```
- name: Patch and reboot servers
hosts: all
vars:
  yum_name: "*"
  yum_state: latest
  yum_securityrepo: yes
  yum_enablerepo: "rhel-?-server-rpms,rhel-?-server-satellite-tools-6.?-rpms"
  yum_disablerepo: "*"
  yum_exclude: ""
tasks:
  - name: upgrade packages via yum
    yum:
      name:{{ yum_name }}
      state:{{ yum_state }}
      security:{{ yum_securityrepo }}
    become: "yes"
    register: yumcommandout
    when:
      - (ansible_facts['distribution_major_version'] == '6') or
        (ansible_facts['distribution_major_version'] == '7')

  - name: display security packages
    debug:
      msg: "security patches for: {{ yumcommandout.changes.updated }}"
    when: yumcommandout.changes is defined

  - name: check to see if we need a reboot
    command: needs-restarting -r
    register: result
    ignore_errors: yes
    changed_when: false #avoid changed

  - name: Reboot Server if Necessary
    command: shutdown -r now "Ansible Updates Triggered"
    become: true
    async: 30
    poll: 0
    when: result.rc is defined and result.rc == 1
```

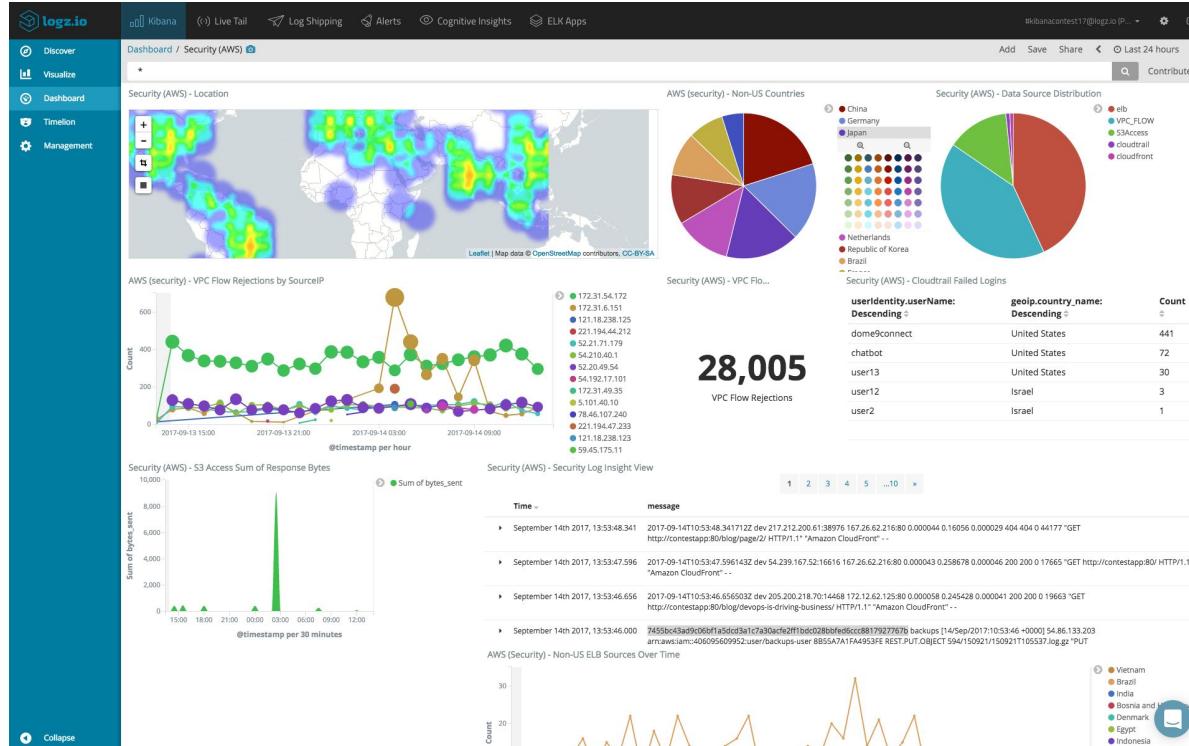


# Monitor: Security Monitoring





# Elastic Security



SIEM at the speed of Elasticsearch



# Falco

- Runtime detection
- Alerts



## Build

- Image Scanning
- Configuration Validation

## Run

- Runtime prevention
- Automated policy creation using ML
- Policy editor and rules library
- Automatic remediation
- Falco Tuning

## Respond

- Incident Response
- Forensics
- Audit



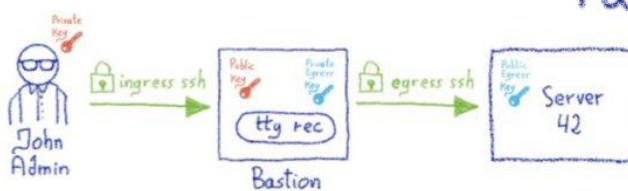
← Continuous Compliance (PCI, NIST, CIS, etc.) →



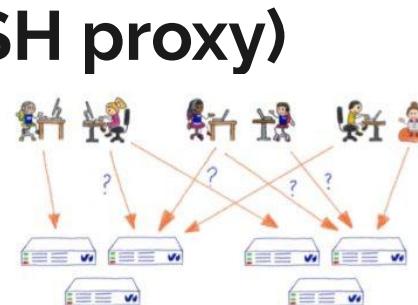
[Kris Nova, Fixing the Kubernetes clusterfuck @FOSDEM](#)

# OVH Bastion (SSH proxy)

The  
 OVHcloud  
Bastion



Part #1



```
slesimpl@the-bastion-2.99.99-rc9.2-ovh1:~$ zdevbst --osh help
*-----*
| THIS IS A PRIVATE COMPUTER SYSTEM, UNAUTHORIZED ACCESS IS STRICTLY PROHIBITED.
| ALL CONNECTIONS ARE LOGGED. IF YOU ARE NOT AUTHORIZED, DISCONNECT NOW.
*-----*
Enter PIN for 'PIV Card Holder pin (PIV_II)':
----- the-bastion-2.99.99-rc9.2-ovh1-----
=> OSH help

> MANAGE YOUR ACCOUNT
- manage your ingress credentials (you->bastion):
  selfListIngressKeys selfAddIngressKey selfDelIngressKey
  selfGenerateIngressKey selfUpdateIngressKey

- manage your egress credentials (bastion->server):
  selfListEgressKeys selfGenerateEgressKey
  selfAddEgressKey selfDelEgressKey
  selfUpdateEgressKey

- manage your accesses to servers:
  selfListAccesses selfAddPersonalAccess selfDelPersonalAccess
  selfUpdatePersonalAccess
  selfListServerAccesses selfAddServerAccess selfDelServerAccess
  selfUpdateServerAccess
```



[Blog article](#) / [Documentation](#) / [Source Code](#)



# Feedback: Secu. Analysis



# AlienVault OTX



Hi David,

A user you are subscribed to (AlienVault) has posted a new pulse:



## Introducing The Jupyter Infostealer/Backdoor

[VIEW PULSE](#)

[SUGGEST EDIT](#)

[SCAN ENDPOINTS](#)

To view the pulse, please visit <https://otx.alienvault.com/pulse/5faf00679c90b876019cc653/>

Click "Embed" on the pulse to insert this pulse in your blog.

You can also [tweet](#) it out to your followers.

Get this updated threat intelligence automatically in your infrastructure using [the OTX API](#)



[OTX: Open Threat Exchange \[EN\]](#)



#cloudest2021

@dadideo



92



# AlienVault OTX



Browse

Scan Endpoints

Create Pulse

Submit Sample

API Integration

All ▾ Search OTX



## Introducing The Jupyter Infostealer/Backdoor



CREATED 2 DAYS AGO by AlienVault | Public | TLP: White

During what began as a routine incident response process, Morphisec has identified (and prevented) a new .NET infostealer variant called Jupyter. Morphisec discovered this variant as part of assisting a higher education customer in the U.S. with their incident response. Jupyter is an infostealer that primarily targets Chromium, Firefox, and Chrome browser data. However, its attack chain, delivery, and loader demonstrate additional capabilities for full backdoor functionality.

REFERENCE: [https://www.morphisec.com/hubfs/eBooks\\_and\\_Whitepapers/Jupyter%20Infostealer%20WEB.pdf](https://www.morphisec.com/hubfs/eBooks_and_Whitepapers/Jupyter%20Infostealer%20WEB.pdf)

TAGS: Jupyter Loader, Infostealer, Backdoor, Academia, Russian Actors, Docx2Rtf, Magix Photo Manager, Jupyter Client, PoshC2

INDUSTRY: Education

MALWARE FAMILIES: PoshC2 - S0378, Jupyter Loader, Jupyter Client

ATT&CK IDS:

T1564 - Hide Artifacts, T1033 - System Owner/User Discovery, T1082 - System Information Discovery, T1140 - Deobfuscate/Decode, T1127 - Trusted Developer Utilities Proxy Execution, T1059.001 - PowerShell, T1055.012 - Process Hollowing, T1036 - Masquerading, T1217 - Browser Bookmark Discovery, T1050.001 - Archive via Utility, T1059.003 - Windows Command Shell, T1547.001 - Registry Run, T1049 - System Network Connections Discovery, T1016 - System Network Configuration Discovery

ENDPOINT SECURITY Scan your endpoints for IOCs from this Pulse!

Indicators of Compromise (39)

Related Pulses (8)

Comments (0)

History (0)



TYPES OF INDICATORS

Show 10 entries

TYPE INDICATOR

ROLE

TITLE

IPv4 91.241.19.21

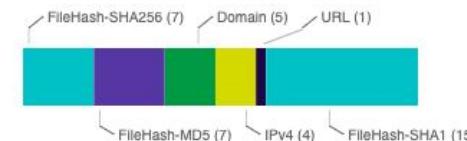
© COPYRIGHT 2020 ALIENVAULT, INC. | LEGAL | STATUS |

## Indicators of Compromise (39)

Related Pulses (8)

Comments (0)

History (0)



## TYPES OF INDICATORS

Show 10 entries

## THREAT INFRASTRUCTURE

Russian Federation (2)

United Kingdom of Great Britain and

## THREAT INFRASTRUCTURE

ROLE

TITLE

IPv4 91.241.19.21

IPv4 45.146.165.219

IPv4 45.146.165.222

IPv4 45.135.232.131

FileHash-SHA1 6ad28e1810eb1be26e835e5224e78e13576887b9



Introducing The Jupyter Infostealer/Backdoor



# SAUCS


[Have an account ?](#)
 [Vulnerabilities \(CVE\)](#)
 [Vendors \(CPE\)](#)
 [Categories \(CWE\)](#)

Search...

[Sign in](#) [Register](#)
**FILTER**

Search
ALL
LOW
MEDIUM
HIGH

130145
total CVE

CVE	Vendors	Products	Updated	CVSS
<a href="#">CVE-2019-2215</a>	<a href="#">1 Google</a>	<a href="#">1 Android</a>	2019-10-16	<span>4.6</span>
A use-after-free in binder.c allows an elevation of privilege from an application to the Linux Kernel. No user interaction is required to exploit this vulnerability, however exploitation does require either the installation of a malicious local...				
<a href="#">CVE-2019-2183</a>	<a href="#">1 Google</a>	<a href="#">1 Android</a>	2019-10-16	<span>2.1</span>
In generateServicesMap of RegisteredServicesCache.java, there is a possible account protection bypass due to a caching optimization. This could lead to local information disclosure with no additional execution privileges needed. User interaction...				
<a href="#">CVE-2019-9533</a>	<a href="#">1 Cobham</a>	<a href="#">1 Explorer 710 Firmware</a>	2019-10-16	<span>10.0</span>
The root password of the Cobham EXPLORER 710 is the same for all versions of firmware up to and including v1.08. This could allow an attacker to reverse-engineer the password from available versions to gain authenticated access to the device.				
<a href="#">CVE-2019-2187</a>	<a href="#">1 Google</a>	<a href="#">1 Android</a>	2019-10-16	<span>2.1</span>
In nfc_ncif_decode_rf_params of nfc_ncif.cc, there is a possible out of bounds read due to an integer underflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for...				
<a href="#">CVE-2019-17420</a>	<a href="#">2 Oisf, Suricata-ids</a>	<a href="#">2 Libhttp, Suricata</a>	2019-10-16	<span>5.0</span>
In OISF LibHTTP before 0.5.31, as used in Suricata 4.1.4 and other products, an HTTP protocol parsing error causes the http_header signature to not alert on a response with a single \vn ending.				
<a href="#">CVE-2019-2184</a>	<a href="#">1 Google</a>	<a href="#">1 Android</a>	2019-10-16	<span>9.3</span>
In PV_DecodePredictedintraDC of dec_pred_intra_dc.cpp, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution with no additional execution privileges needed. User interaction is needed for...				



[Site Web de SAUCS](#)

# SAUCS / Vue d'une CVE

CVE-2019-2215



Saucs / Vulnerabilities (CVE) / CVE-2019-2215

**A** use-after-free in binder.c allows an elevation of privilege from an application to the Linux Kernel. No user interaction is required to exploit this vulnerability, however exploitation does require either the installation of a malicious local application or a separate vulnerability in a network facing application. Product: AndroidAndroid ID: A-141720095

Published : 2019-10-11 19:15

Updated : 2019-10-16 17:53



ACCESS VECTOR	LOCAL	+
ACCESS COMPLEXITY	LOW	+
AUTHENTICATION	NONE	+

CONFIDENTIALITY IMPACT	PARTIAL	+
INTEGRITY IMPACT	PARTIAL	+
AVAILABILITY IMPACT	PARTIAL	+

CPE (1) Tree view

Vendor	Product	Version	URI
Google	Android	-	cpe:/o:google:android:-

CWE

ID	Name	Description	Links	CVE
CWE-416	Use After Free	Referencing memory after it has been freed can cause a program to crash, use unexpected values, or execute code.		

# CERT-FR (Flux RSS)

[Menaces et incidents](#)

CERT-FR

PUBLICATIONS ▾ SCANS ARCHIVES ▾

RÉSEAU DES CSIRT ▾ RECRUTEMENT CONTACT À PROPOS



## MENACES ET INCIDENTS

### LE MALWARE-AS-A-SERVICE EMOTET

CERTFR-2020-CTI-010 • Publié le 2 novembre 2020

Observé pour la première fois en 2014 en tant que cheval de Troie bancaire, Emotet a évolué vers une structure modulaire à partir de 2015. Depuis 2017, Emotet ...

### 🇬🇧 DEVELOPMENT OF THE ACTIVITY OF THE TA505 CYBERCRIMINAL GROUP

CERTFR-2020-CTI-009 • Publié le 27 août 2020

The intrusion set TA505 has been active since at least 2014 when it initially stole financial information through the use of Dridex and mass distributed ransomwares. It evolved and ...

### 🇬🇧 THE MALWARE DRIDEX: ORIGINS AND USES

CERTFR-2020-CTI-008 • Publié le 17 juillet 2020

Surfacing in June 2014 as a variant of the banking trojan Bugat, Dridex is a malware which has evolved a lot since then in terms of functionalities and uses. This report provides ...



# Lifecycle: Decommission



# Planification (LTS/Migration/EoL)

**techradar.pro**

IT INSIGHTS FOR BUSINESS

US Edition



PAYMENTS INDUSTRY INTELLIGENCE  
**Payments**  
Cards & Mobile



News

Security

Web hosting

VPN

Website builder

Resources

NEWS

PUBLICATIONS

RESEARCH

CONSULTING

CONFERENCES / ADVERTISE / WEBINARS

HOME ◉ DAILY NEWS ◉ ATM MIGRATION TO WINDOWS 10 – THE TIME IS NEAR!

Home > News > Computing

## ATM security still running Windows XP

By Anthony Spadafora November 15, 2018

New study reveals ATM security is mostly for show

New research from Positive Technologies has revealed that ATM machines are vulnerable to a number of basic attack techniques that could allow hackers to steal thousands in cash.

The company's researchers studied over two dozen different models of ATMs and discovered that almost all of them are vulnerable to network or local access attacks that would allow hackers to obtain money from them illegally.

Positive Technologies' study had its researchers try to penetrate 26 machines from various manufacturers and service providers.

The researchers found that 15 of the ATMs were running Windows XP, 22 were vulnerable to a "network spoofing" attack, 18 were vulnerable to 'black box' attacks, 20 could be forced to exit kiosk mode via USB or PS/2 and 24 had no data encryption in place on their hard drives.

## ATM migration to Windows 10 – the time is near!

BY ALEX ROLFE

DECEMBER 11, 2019

DAILY NEWS

SHARE:



2,903 VIEWS

The banking sector will face a big ATM migration challenge in 2020. Microsoft made the official announcement: Windows 7 (operating system for many ATMs) extended support will end on January 14, 2020. Consequently, all banks have to update their entire ATM network by installing a new operating system caring about data security.

There are about 3.2 million ATMs in the world. They are used daily by billions of people, but only a few know that most ATMs work on the Windows operating system.

A lot of ATMs around the globe are still running Windows XP embedded, long after Microsoft ceased support with security and stability patches. Support for Windows XP was discontinued in 2014, which means that since then the Microsoft Company has not rolled out any security updates for this Windows version.



ATM migration to Windows 10 – the time is near!

In June 2018, The Central Bank of India issued a statement saying that all ATMs in the country should be updated from Windows XP to the newer platform by December 2019. It is estimated that about 50% of ATMs use Windows XP operating system.



#cloudest2021

@dadideo



98



# Synthèse



# DevSecOps Toolbox

- Secure Coding
  - [Linters](#), [gosec](#), [npm-audit](#), [GitGuardian](#), [42Crunch](#)
- Security as Code
  - [Cilium](#) (Network), [gVisor/Kata](#) (Sandbox), [Istio/maesh](#) (SSL)
- SAST / DAST / IAST
  - [SonarQube](#), [Gitlab SAST/GitHub](#), [Clair/Anchore/Dagda](#) (CVE)
- Pentest
  - [Parrot](#), [Kali OS](#), [YesWeHack](#), [Yogosha](#), [Burp Suite/SuperTruder/ffuf](#), [OWASP ZAP](#)
- Digital signature / Secure Transfer
  - [Notary](#), [JFrog Artifactory](#)
- Security Configuration, Security Scan
  - [Argo+Vault](#), [OpenSCAP](#)
- Security Patching, Security Audit
  - [Puppet](#), [Chef](#), [Ansible Playbook/AWX](#) ou [RedHat Tower](#)
- Security Monitoring
  - [Elastic Security](#), [Falco](#), [OVH Bastion](#)
- Security Analysis
  - [Saucs](#), [AlienVault OTX](#)

And more... (not exhaustive) 😊



#cloudest2021

@dadideo



100



Pause pour les questions





#cloudest2021

@dadideo



101



# Contexte



# Pourquoi ?

## OWASP TOP 10 – 2013

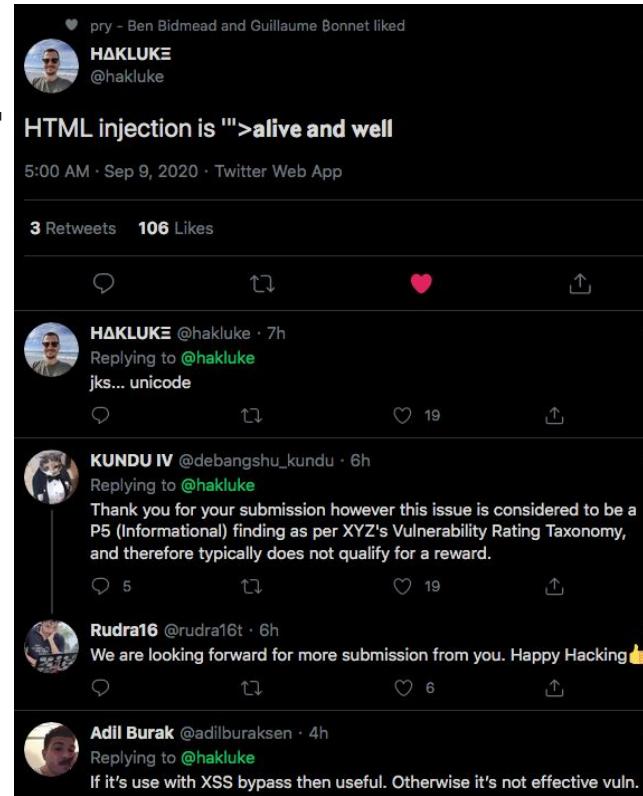
- A1 – Injection
- A2 – Broken Authentication and Session Management
- A3 – Cross-Site Scripting (XSS)
- A4 – Insecure Direct Object References **[Merged + A7]**
- A5 – Security Misconfiguration
- A6 – Sensitive Data Exposure
- A7 – Missing Function Level Access Control **[Merged + A4]**
- A8 – Cross-Site Request Forgery (CSRF)
- A9 – Using Components with Known Vulnerabilities
- A10 – Unvalidated Redirects and Forwards

## OWASP TOP 10 – 2017

- A1 – Injection
- A2 – Broken Authentication
- A3 – Sensitive Data Exposure
- A4 – XML External Entities (XXE) **[NEW]**
- A5 – Broken Access Control **[MERGED]**
- A6 – Security Misconfiguration
- A7 – Cross-Site Scripting (XSS)
- A8 – Insecure Deserialization **[NEW, COMMUNITY]**
- A9 – Using Components with Known Vulnerabilities
- A10 – Insufficient Logging & Monitoring **[NEW, COMMUNITY]**

Source: [https://www.owasp.org/images/7/72/OWASP\\_Top\\_10-2017\\_%28en%29.pdf.pdf](https://www.owasp.org/images/7/72/OWASP_Top_10-2017_%28en%29.pdf.pdf)

# I Will Survive Gloria Gaynor



A screenshot of a Twitter thread from user @hakluke. The thread consists of five tweets:

- HAKLUKE** (@hakluke) · 7h ago  
HTML injection is ">alive and well"  
5:00 AM · Sep 9, 2020 · Twitter Web App  
3 Retweets 106 Likes
- HAKLUKE** (@hakluke) · 7h ago  
Replying to @hakluke  
jk... unicode  
19 Likes
- KUNDU IV** (@debangshu\_kundu) · 6h ago  
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.  
19 Likes
- Rudra16** (@rudra16t) · 6h ago  
We are looking forward for more submission from you. Happy Hacking!  
6 Likes
- Adil Burak** (@adilburaksen) · 4h ago  
Replying to @hakluke  
If it's use with XSS bypass then useful. Otherwise it's not effective vuln.



<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 selon GARTNER

Développement logiciel

**90%**

DevSecOps  
(+40% 2019)

Projets IT

**25%**

DevOps  
(+10% 2019)



Gartner/Techwire



#cloudest2021

@dadideo



106



# Conseils

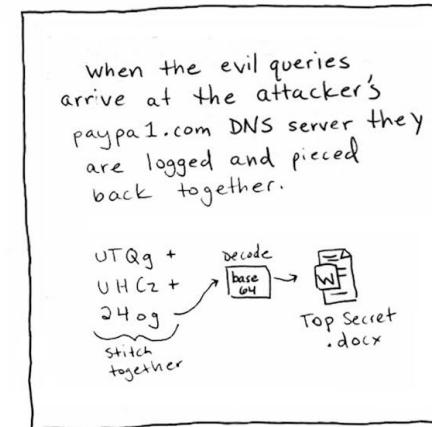
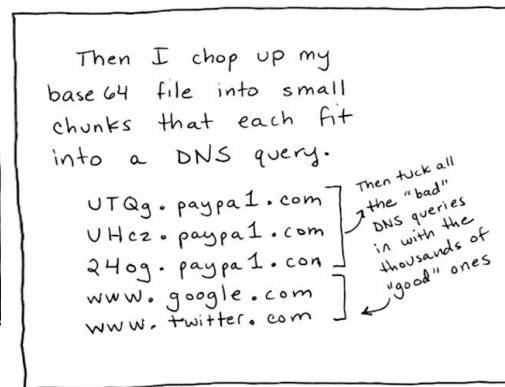
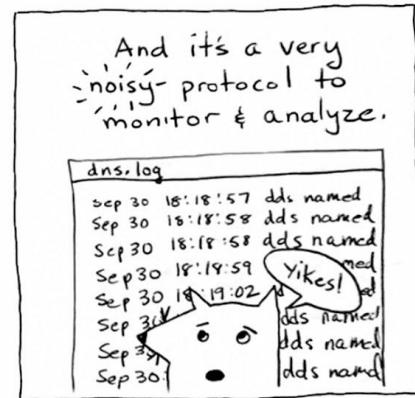
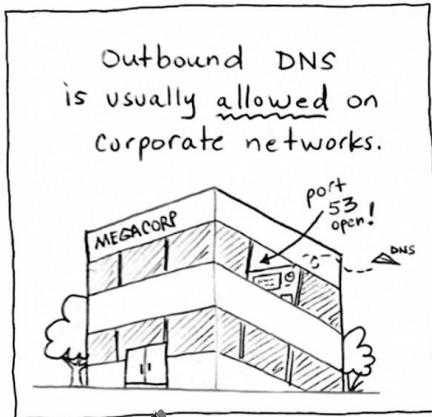
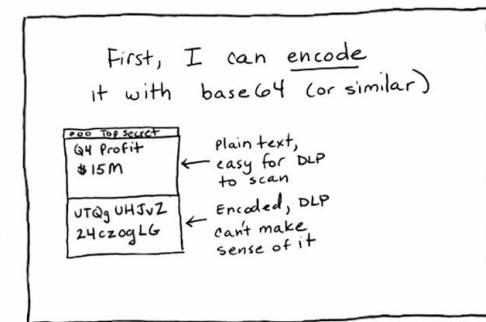
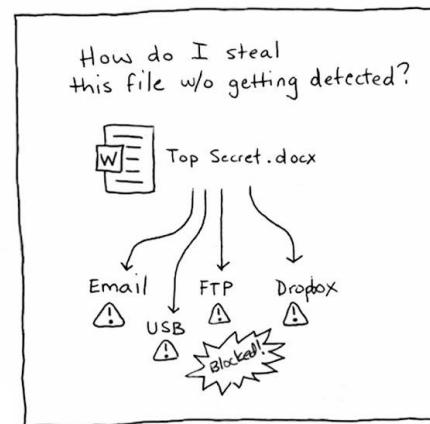
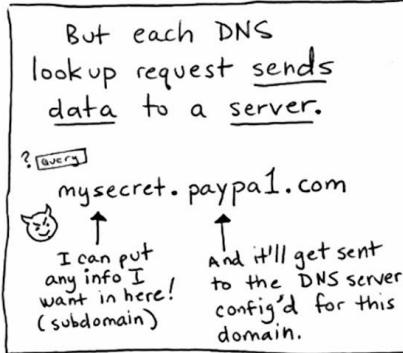
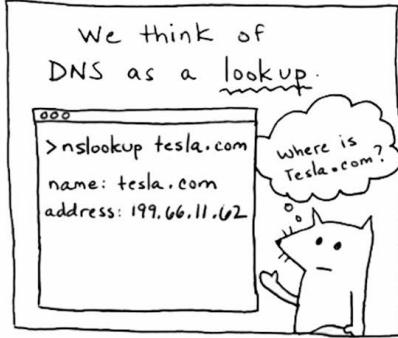




# Attention au traffic sortant



Introduction à DNSSEC



Exfiltration DNS @Rob Sobers

# Attention au 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

# 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



[What's Your Security Maturity Level? \[EN\]](#)

# Maintenez vos systèmes à jour



**Ben Hawkes**  
@benhawkes

...

Apple have fixed three issues reported by Project Zero that were being actively exploited in the wild.

CVE-2020-27930 (RCE), CVE-2020-27950 (memory leak), and CVE-2020-27932 (kernel privilege escalation). The security bulletin is available here:



About the security content of iOS 14.2 and iPadOS 14.2  
This document describes the security content of iOS 14.2 and iPadOS 14.2.  
[support.apple.com](https://support.apple.com)

7:46 PM · Nov 5, 2020 · Twitter Web App



[@benhawkes | Apple Security Update](#)



#cloudest2021

@dadideo



111



# Audits





---

# Certifications

## Normatives

- ISO/CEI 27001, 27017, 27018
- PCI
- HITRUST
- CSA STAR
- HDS

## Robustesse logiciel/SI

- CSPN
- CC EAL 3+
- CC EAL 4+





---

# Qualifications

Des services SSI

- SecNumCloud
- PSCE
- PRIS
- PDIS
- PASSI
- PSHE



[Site web de l'ANSSI](#)





#cloudest2021

@dadideo



114



# Hackers





### 3.3.3 Niveau de l'attaquant

Cette grille est nécessaire pour l'évaluation de la vraisemblance. La classification suivante est proposée pour le niveau de l'attaquant.

	Niveau	Qualificatif	Description/Exemples
Attaquant	1	Non ciblé	Virus, robots...
	2	Hobbyiste	Personnes avec des moyens très limités, pas nécessairement de volonté de nuire.
	3	Attaquant isolé	Personne ou organisme avec des moyens limités mais avec une certaine détermination (employé licencié, par exemple).
	4	Organisation privée	Organisme aux moyens conséquents (terrorisme, concurrence déloyale, par exemple).
	5	Organisation étatique	Organisme aux moyens illimités et à la détermination très forte.



# Preuve : de récentes attaques contre des labos

Coronavirus : les hackers russes et nord-coréens s'attaquent aux projets de vaccin

© 16/11/2020 à 09h21



Détectées par Microsoft, ces attaques auraient été réalisées par le groupe russe Strontium, alias APT28 ou FancyBear, et par les groupes nord-coréens Zinc, alias Hidden Cobra, et Cerium. L'éditeur n'a pas détaillé les noms des entreprises ciblées, mais a indiqué qu'elles se situait en France, au Canada, en Inde, en Corée du Sud et aux États-Unis.

Des laboratoires dans le monde entier ont été ciblés, dont au moins un en France. La plupart des attaques ont été bloquées, mais certains pirates ont réussi à pénétrer des systèmes.



[01net - Hackers contre les projets de vaccin / ArsTechnica \[EN\]](#)

# Rappelez-vous: Les hackers n'en ont rien à foutre

- À propos du scope de votre projet
- Il est géré par une tierce partie / sous-traitant
- C'est un système ancien (Legacy)
- TPCM / " Touche pas ! C'est magique "
- C'est "trop critique pour être réparé"
- A propos de vos périodes de maintenance
- A propos de votre budget
- Vous l'avez toujours fait de cette façon
- À propos de votre date de mise en service
- Il s'agit seulement d'un pilote/PoC
- À propos des accords de non-divulgation
- Ce n'était pas une exigence dans le contrat
- C'est un système interne
- Il est vraiment difficile de modifier / changer
- Vous n'êtes pas sûr de savoir comment y remédier
- Il doit être remplacé
- C'est géré dans le Cloud
- À propos de votre inscription au registre des risques
- L'éditeur ne prend pas en charge cette configuration
- C'est une solution provisoire
- Il est conforme à [insérer la norme ici]
- Il est crypté sur disque
- Le rapport coût-bénéfice ne scale pas
- "Personne d'autre ne pouvait le comprendre"
- Vous ne pouvez pas expliquer le risque au "Business"
- Vous avez d'autres priorités
- Sur votre foi dans la compétence de vos utilisateurs internes
- Vous n'avez pas de justification commerciale
- Vous ne pouvez pas montrer le retour sur investissement
- Vous avez sous-traité ce risque
- C'était à la mode [insérer la technologie hype ici].
- De vos certifications





---

# Analogie

« Nul n'est censé ignorer la loi »





---

# Ma devise

« Nul développeur n'est censé ignorer la sécurité »





#cloudest2021

@dadideo



120



---

# Merci pour votre attention !



Jungfraujoch, Switzerland (by [Erol Ahmed](#))  
The pictures are from [Unsplash](#)



#cloudest2021

@dadideo



121



## 🍻🍻 R.O.T.I :

Go to [www.menti.com](http://www.menti.com) and use the code 4671 4382





# 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



## 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



## 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



The state of open  
source security - 2019



---



## Pour aller plus loin

- [Sophia Security Camp 2019](#)
- [ANSSI](#) (Atelier [Sécurité Agile](#), Livre Sécurité au déploiement de conteneurs [Docker](#))
- [TV5 Monde Analyse d'Incident](#), ANSSI (SSTIC 2017)
- [10 leçons sur les 10 plus grosses fuites de données](#), de Adrien Pessu (JSC 2020)
- [La Cryptographie en 55' chrono](#) de m4dz (SnowCamp2020)
- [Sécurité du Cloud](#), de Eric Briand (RemoteClazz 2020)
- [La nuit tous les hackers sont gris](#) (Fiction écrite par Vincent Hazard, 2019)



#cloudest2021

@dadideo



124



## Vouchers



### ESSAI GRATUIT AI NOTEBOOKS

Profitez d'un crédit offert\* de 70€ pour démarrer votre notebook Jupyter ou VS Code en quelques minutes ! **Code : AI-NTBK21**

[En profiter](#)



**ESSAI GRATUIT PUBLIC CLOUD**  
Profitez maintenant de 30 € de crédit offert\* avec le code : CLOUD  
[Commencer](#)

OVHcloud  
openstack.



#cloudest2021

@dadideo



125



---

# Encore merci !

N'oubliez pas de me donner votre avis sur:  
<https://s.42l.fr/cloudest2021>

Slides: <https://davidaparicio.gitlab.io/website/>

Merci



# Rappelez-vous: Les hackers n'en ont rien à foutre

- À propos du scope de votre projet
- Il est géré par une tierce partie / sous-traitant
- C'est un système ancien (Legacy)
- TPCM / " Touche pas ! C'est magique "
- C'est "trop critique pour être réparé"
- A propos de vos périodes de maintenance
- A propos de votre budget
- Vous l'avez toujours fait de cette façon
- À propos de votre date de mise en service
- Il s'agit seulement d'un pilote/PoC
- À propos des accords de non-divulgation
- Ce n'était pas une exigence dans le contrat
- C'est un système interne
- Il est vraiment difficile de modifier / changer
- Vous n'êtes pas sûr de savoir comment y remédier
- Il doit être remplacé
- C'est géré dans le Cloud
- À propos de votre inscription au registre des risques
- L'éditeur ne prend pas en charge cette configuration
- C'est une solution provisoire
- Il est conforme à [insérer la norme ici]
- Il est crypté sur disque
- Le rapport coût-bénéfice ne scale pas
- "Personne d'autre ne pouvait le comprendre"
- Vous ne pouvez pas expliquer le risque au "Business"
- Vous avez d'autres priorités
- Sur votre foi dans la compétence de vos utilisateurs internes
- Vous n'avez pas de justification commerciale
- Vous ne pouvez pas montrer le retour sur investissement
- Vous avez sous-traité ce risque
- C'était à la mode [insérer la technologie hype ici].
- De vos certifications



# Rappelez-vous: Hackers don't give a shit:

- About your project's scope
- It's managed by a third party
- It's a legacy system
- It's "too critical to patch"
- About your outage windows
- About your budget
- You've always done it that way
- About your Go-Live Date
- It's only a pilot/proof of concept
- About Non-Disclosure Agreements
- It wasn't a requirement in the contract
- It's an internal system
- It's really hard to change
- It's due for replacement
- You're not sure how to fix it
- It's handled in the Cloud
- About your Risk Register entry
- The vendor doesn't support that configuration
- It's an interim solution
- It's [insert standard here] compliant
- It's encrypted on disk
- The cost benefit doesn't stack up
- "Nobody else could figure that out"
- You can't explain the risk to "The Business"
- You've got other priorities
- About your faith in the competence of your internal users
- You don't have a business justification
- You can't show Return on Investment
- You contracted out that risk

